



marque déposée

NOMBRES &
PROBABILITES
Mercier Dany-Jack
TC2

le Calligraphe

cahier _____

école _____

classe _____

nom _____



N° 103

TC2

NOMBRES & PROBABILITES

LEÇONS

n°1

COURS DE TERMINALE C

DE MME J. MANOTTE

reçu et présenté par D.-J. MERCIER

1974 - 75

19.9

1

Ensemble \mathbb{N} des entiers naturels

(livre p 17)

 $\exists \mathbb{N}$ tel que1°) $+$ et \times sont des lois internes dans \mathbb{N} . (voir propriétés)2°) \leq exprime une relation d'ordre dans \mathbb{N} .

L'ordre est total :

 $\forall (x, y) \in \mathbb{N}^2$, nous avons $x \leq y$ ou $y \leq x$ $x \in \mathbb{N}, y \in \mathbb{N}, z \in \mathbb{N}$ $x \leq y \implies x + z \leq y + z$ (compatibilité)3°) $\forall A, A \subset \mathbb{N}$ $A \neq \emptyset, \exists \alpha, \alpha \in A / \forall x \in A, \alpha \leq x$ 2°: \mathbb{N} a 0 comme plus petit élément.4°) $\forall A \subset \mathbb{N}, A \neq \emptyset$ et A majorée, $\exists \beta \in A / \forall x \in A, \beta \geq x$.

(cf p 18)

2°: \mathbb{N} n'a pas de plus grand élément.

Raisonnement par récurrence

Soit $A \subset \mathbb{N} / 0 \in A$ et : $\forall x \in A \implies x+1 \in A$ Alors $A = \mathbb{N}$

Deuxième forme.

Soit $A = \{x / x \in \mathbb{N}, P(x) \text{ vraie}\}$

Si $\begin{cases} P(0) \text{ est vraie.} \\ P(n) \vdash P(n+1) \end{cases}$

avec $n \in A$

Alors $P(n)$ est générale = vraie $\forall n \in \mathbb{N}$.

Démonstration

$A \subset \mathbb{N}$; $B = \bigcap_{\mathbb{N}} A = \mathbb{N} - A$

Soit $y \in B$; $B = \{y, y \in \mathbb{N} / y \notin A\}$

Si $B \neq \emptyset$, $\exists y$ (\exists = il existe au moins)

B est alors une partie non vide de \mathbb{N} ; $\exists y_0$, le plus petit élément de B . $y_0 \neq 0$ car $0 \in A$ et $y_0 \in B$

Donc, $\exists (y_0 - 1)$

$y_0 - 1 \in A$ car y_0 est le p.p. élément de B .

Gr, $y_0 - 1 \in A \vdash (y_0 - 1) + 1 \in A$ (voir énoncé)
 $\vdash y_0 \in A$

Gr, $A \cap B = \emptyset$, d'où contradiction : c'est donc que $B = \emptyset$ ($\nexists y$) $\vdash A = \mathbb{N}$

Exemple.

Montrer que :

$$1 + 3 + 5 + \dots + (2n-1) = n^2 \quad : P(n)$$

1° $P(1)$ est vraie car $1=1^2$

2° $P(n) \rightarrow P(n+1)$?

Si $1+3+5+\dots+(2n-1)=n^2$,

alors est-ce que.

$$\underbrace{1+3+5+\dots+(2n-1)}_{n^2} + (2n+1) = (n+1)^2 \quad ?$$

$$= n^2 + 2n + 1$$

Conclusion.

$P(n)$ est vraie $\forall n \in \mathbb{N}^*$

26.9

Remarque.

Si $0 \notin A \rightarrow$ Si $P(0)$ non vraie,

Si, de plus, le 1^{er} élément de \mathbb{N} pour lequel $P(x)$ est vraie est \boxed{a} .

$$\begin{cases} P(a) \text{ vraie} \\ \text{et} \\ P(x) \rightarrow P(x+1) \text{ vraie} \end{cases}$$

Alors $P(x)$ vrai $\forall x \in \mathbb{N} - \{0, 1, \dots, a-1\} = A$

1° Propriété d'Archimède:

$$a \in \mathbb{N}, b \in \mathbb{N}^*$$

$$(a+1)b = ab + b$$

$$\begin{cases} (a+1)b > ab & (\text{car } b > 0) \\ ab \geq a & (\text{car } b \geq 1) \end{cases}$$

donc:

$$(a+1)b > a$$

$$a < (a+1)b$$

$$\boxed{\exists k \in \mathbb{N}}; a < kb$$

L'ensemble des entiers kb que k n'est pas vide puisque $a+1$ est l'un d'entre eux.

Il y a un plus petit élément dans cette partie $\neq \emptyset$ de \mathbb{N} .

On l'appelle $q+1$. Son prédécesseur dans \mathbb{N} est q et ne vérifie pas $a < kb$

nous avons donc: $a \geq qb$

On rappelle $a < (q+1)b$

$$(1) \quad \boxed{qb \leq a < (q+1)b}$$

$$\text{ex: } 25 \times 5 \leq a < 26 \times 5$$

$25 = q =$ quotient entier de a par 5 si et seulement si $a = 125$, ou 126, ou 127, ou 129.

Règle de la division euclidienne de a par b :

$$\text{c'est } r \in \mathbb{N} \quad / \quad a = bq + r$$

$$\underline{r = a - bq} \quad ; \quad r \geq 0 \quad \text{et} \quad r < b$$

$$r = a - bq$$

$$0 \leq r < b$$

(2)

$$\exists a = bq + r$$

Les propriétés (1) et (2) sont équivalentes.

27.9

2°/ écriture d'un entier naturel n dans un système de numération de base x .

Le principe est le même que si $x = 10$.

a) Si $n < x$, on écrit n avec un symbole unique appelé "chiffre" (ou un caractère)

b) Si $n \geq x$, on écrit n à l'aide de chiffres rangés dans un ~~nombre~~ ordre tel que : à droite, le nombre des unités simples.

à sa gauche, le nombre des unités du 2^e ordre, chacune d'elles renfermant x unités simples.

x encore à sa gauche, le nombre des unités du 3^e-ordre, chacune renferment x unités du 2^e-ordre.

* ...

Pratique

- 1° $n < x$, on convient d'un choix de x caractères
- * $x \leq 10$, on utilise les chiffres habituels.
- * $x > 10$, on en introduit de nouveaux en gardant les dix premiers.

ex: $x = \text{douze}$; $\{0, 1, \dots, 9, \alpha, \beta\}$

2° $n \geq x$, on div $\exists (q_1, r_1) /$

$$n = \boxed{q_1} x + \boxed{r_1}, \quad 0 \leq r_1 < x \quad (x \neq 0)$$

* Si $q_1 < x$, on convient d'écrire:

$$n = \overline{q_1 r_1}$$

* Si $q_1 \geq x$, on le divise à son tour par x :

$$q_1 = q_2 x + r_2 \quad 0 \leq r_2 < x$$

* Si $q_2 < x$, on convient d'écrire:

$$n = \overline{q_2 r_2 r_1}$$

* Si $q_2 \geq x$,

$$q_2 = q_3 x + r_3 \quad 0 \leq r_3 < x$$

et ainsi de suite.

$$\text{et } n = \overline{q_p r_p \dots r_1}$$

Résumé

$$\begin{array}{lll}
 & n = q_1 x + r_1 & 0 \leq r_1 < x \\
 \times x & q_1 = q_2 x + r_2 & 0 \leq r_2 < x \\
 \times x^2 & q_2 = q_3 x + r_3 & 0 \leq r_3 < x \\
 & \dots & \\
 \times x^{p-1} & q_{p-1} = q_p x + r_p & 0 \leq r_p < x \\
 \times x^p & q_p = 0 x + q_p & 0 < q_p < x
 \end{array}$$

Si $q_p = r_{p+1} \neq 0$

On ajoute membre à membre les égalités obtenues après les multiplications précédentes:

$$n = r_1 + r_2 x + r_3 x^2 + \dots + r_p x^{p-1} + \underbrace{q_p x^p}_{r_{p+1}}$$

$n = \underbrace{r_{p+1} x^p}_{\text{}} + \underbrace{r_p x^{p-1}}_{\text{}} + \dots + \underbrace{r_2 x}_{\text{}} + \underbrace{r_1}_{\text{}}$	donc
$n = \overline{r_{p+1} r_p \dots r_2 r_1}$	donc

exemple

Si $x = 2$ (base deux).

$$n = 1001011101$$

$$\begin{aligned} n &= 1x^{10} + 1x^7 + 1x^5 + 1x^4 + 1x^3 + 1x^2 + 1 \\ &= 1024 + 128 + 32 + 16 + 8 + 4 + 1 \\ n &= 1213 \quad (\text{base dix}) \end{aligned}$$

Représentation de n en base x dans la base x .

$$x^1 = 1x^1 + 0$$

$$x = \overline{10}, \text{ en base } x, \forall x \in \mathbb{N} - \{0, 1\}$$

$$x^2 = \overline{100}$$

Unicité de l'écriture de $n \in \mathbb{N}$ dans un système de

$$\exists! (q_1, r_1); \exists! (q_2, r_2); \dots$$

De plus, la position des restes successifs est imposée.

Remarque

$$x = \overline{10} \quad \forall x$$

$$x^2 = \overline{100}$$

$$x^n = \overline{100 \dots 00}$$

$n+1$ caractères
mais n zéros.

2.10

3

Étude de l'anneau $(\mathbb{Z}, +, \times)$ Il s'agit de $(\mathbb{Z}, +, \times)$ 1° $(\mathbb{Z}, +)$ groupe commutatif.2° \times est associative.3° \times est distributive sur4° \mathbb{Z} est un anneau commutatif5° \mathbb{Z} " " unitaire} \mathbb{Z} est un anneau.Étude de $E = n\mathbb{Z}$ $n \in \mathbb{N}$

$$E = \{x \in \mathbb{Z} / \exists q \in \mathbb{Z}, x = nq\}$$

3.10

 $(E, +)$ est un sous-groupe de $(\mathbb{Z}, +)$:1° $E \neq \emptyset$ car $0 = n \cdot 0$ donc $0 \in n\mathbb{Z}$ 2° $x \in n\mathbb{Z}$ et $x' \in n\mathbb{Z}$

$$x - x' = nq - nq' = n(q - q')$$

$$q \in \mathbb{Z}, q' \in \mathbb{Z} \quad q - q' \in \mathbb{Z}$$

$$[q + (-q')] \in \mathbb{Z}$$

$$\exists q - q' = Q \in \mathbb{Z} / x - x' = nQ$$

$$x - x' \in n\mathbb{Z}$$

Inversement, soit E un sous-groupe de $(\mathbb{Z}, +)$.1° Si $E = \{0\}$, il peut se mettre sous la forme

$$E = n\mathbb{Z}$$

2°) Si $E \neq \{0\}$, alors $\exists \underset{\neq 0}{x} \in E$, $\exists (-x) \in E$
 Des deux: x et $-x$, l'un est positif. L'ensemble
 des entiers positifs inclus dans E n'est pas vide, or
 $A \neq \emptyset$ et $A \subset \mathbb{N} \mapsto \exists$ plus petit élément dans
 soit n cet élément.

* Considérons $E' = n\mathbb{Z}$ ($n \in \mathbb{N}^*$)
 $n\mathbb{Z} \subset E$?

$$\begin{array}{l} x = \underbrace{nq}_{\in E} \\ \in E \end{array}$$

$$\text{Si } q > 0, \quad x = \underbrace{n + n + \dots + n}_{\substack{q \text{ termes} \\ \in E \text{ (+ interne dans } E)}} \in E$$

$$\text{Si } q < 0, \quad -q = q' > 0$$

$$x = nq = \underbrace{(-n)q'}_{\in E > 0} \text{ et } x \in E \text{ aussi.}$$

$$\text{Si } q = 0, \quad x = 0 \in E.$$

$$\text{Donc } \underline{n\mathbb{Z} \subset E}$$

* On n'aura $n\mathbb{Z} = E$ que si, de plus $E \subset n\mathbb{Z}$

$$\text{Si } x \in E, \quad x = nq + r \quad 0 \leq r < \underbrace{n}_{\text{diviseur}}$$

$$\text{Si } \underline{r} > 0, \quad r = \underbrace{x}_{\in E} - \underbrace{nq}_{\in E} \notin n\mathbb{Z} \subset E$$

Donc $n \in E$

Or, n est le plus petit élément ^{strictement} positif de E . Donc :
incompatibilité avec $0 < n < n$.

Donc $n = 0 \mid x = nq \in n\mathbb{Z}$

Donc $E \subset n\mathbb{Z}$

* Conclusion

— "Tous les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $(n\mathbb{Z}, +)$."

Sous-anneaux de $(\mathbb{Z}, +, \times)$

Ce sont des sous-groupes de $(\mathbb{Z}, +)$ donc des $n\mathbb{Z}$.

Tous les $n\mathbb{Z}$ sont-ils anneaux ? oui si et seulement si

$\forall x \in n\mathbb{Z}, \forall x' \in n\mathbb{Z}$, alors $x \times x' \in n\mathbb{Z}$

Or, $x \cdot x' = nq \cdot nq' = n(\underbrace{q \cdot q'}_{\in \mathbb{Z}}) = nQ$

soit $x' \in n\mathbb{Z}$.

— "Tous les sous-anneaux de $(\mathbb{Z}, +, \times)$ sont les $n\mathbb{Z}$ "

4.10

Définition d'un idéal d'un anneau commutatif

$(A, +, \times)$ = anneau commutatif

\mathcal{I} = idéal de A si et seulement si :

* $(\mathcal{I}, +)$ = sous-groupe

* $\forall x \in \mathcal{I}, \forall y \in A, \quad x \times y \in \mathcal{I}$

On dit que \mathcal{I} est (\mathbb{Z} -propriété) une partie "multiplicativement permise" de A .

Résumé :

* $\forall (x, y) \in \mathcal{I}^2, \quad x - y \in \mathcal{I}$

* $\forall x \in \mathcal{I}, \forall z \in A, \quad x \times z \in \mathcal{I}$

Cas où $A = \mathbb{Z}$

Les idéaux de \mathbb{Z} sont évidemment les $n\mathbb{Z}$ car

1°) $n\mathbb{Z}$ = sous-groupe de \mathbb{Z}

2°) $\forall x = nq, \quad q \in \mathbb{Z}$

$$\forall z \in \mathbb{Z} \quad xz = n \underbrace{(qz)}_{\in \mathbb{Z}}$$

$$xz = nq' \in n\mathbb{Z}$$

exemples

1) a est divisible par $b \neq 0$

2) a est multiple de b .

3) b divise a : $b|a$

4) b est diviseur de a .

Cela signifie : $a \in \mathbb{Z}$, $b \in \mathbb{Z}$,

$$\exists q \in \mathbb{Z} / a = bq$$

5) $a\mathbb{Z} \subset b\mathbb{Z}$

Ex. $3 \mid 15$; tout multiple de 15 est multiple de 3 ; la réciproque est fausse.

$$b \mid a \mapsto (a) \subset (b)$$

$$(a) = a\mathbb{Z}$$

$$(b) = b\mathbb{Z}.$$

(a) se lit "Idéal de a ".

1° Division euclidienne de $a \in \mathbb{Z}$ par $b \in \mathbb{N}^*$

$\alpha)$ Si $a \geq 0$ ($a \in \mathbb{N}$), déjà vu:

$$bq \leq a < b(q+1)$$

ou: $a = bq + r \quad 0 \leq r < b$

$\beta)$ Si $a \leq 0$ ($a \in \mathbb{Z}_-$); $a = -a' \quad a' \in \mathbb{N}$

$$bq' \leq a' < b(q'+1)$$

* si $a' = bq'$, alors $a = -a' = -bq' = b \underbrace{(-q')}_{\in \mathbb{Z}}$
donc $a = b \underbrace{(-q')}_{\text{quotient de } a \text{ par } b.}$

ex: $a = -35$; $b = 7 \quad -35 = 7 \times \underbrace{(-5)}_{-q'}$

$-q' = q = \text{quotient de } a \text{ par } b.$

* $a' \neq bq'$

$$bq' < a' < b(q'+1)$$

$$-b(q'+1) < \underbrace{-a'}_a < -bq'$$

$$-b(q'+1) < a < -bq'$$

$$b \underbrace{[-(q'+1)]}_q < a < b \underbrace{(-q')}_{q+1}$$

$$bq < a < b(q+1)$$

q est le quotient entier de a par b .

$$\text{ex: } 7 \times \boxed{-6} < \underbrace{-37}_a < \underbrace{7 \times (-5)}_b$$

$$-37 = 7(-6) + \underbrace{5}_n$$

$$n \geq 0, \quad n < 7$$

$$a = bq + n \quad 0 \leq n < b$$

2° Relation d'équivalence dans \mathbb{Z} .

$$\forall (x, y) \in \mathbb{Z}^2, \quad x \mathcal{R} y \iff x - y \in n\mathbb{Z}$$

$$\text{ex: } n = 5, \quad x = -37$$

$$y = -57$$

$$x - y = -37 + 57 = 20 \in n\mathbb{Z}$$

$$x - y \in 5\mathbb{Z} \iff x \mathcal{R} y.$$

$$* \quad \forall x \in \mathbb{Z} \quad x \mathcal{R} x?$$

$$x \mathcal{R} x \iff x - x \in n\mathbb{Z}$$

$$\text{Or } x - x = 0 \in n\mathbb{Z}, \text{ oui.}$$

$$* \quad \forall (x, y) \in \mathbb{Z}^2, \quad x \mathcal{R} y \iff y \mathcal{R} x?$$

$$x \mathcal{R} y \iff x - y \in n\mathbb{Z}$$

$$(n\mathbb{Z}, +) = \text{groupe} \quad \vdash \quad y - x \in n\mathbb{Z}.$$

$$\vdash \quad y \mathcal{R} x$$

$$\forall (x, y, z) \in \mathbb{Z}^3.$$

$$\left. \begin{array}{l} x \mathcal{R} y \\ y \mathcal{R} z \end{array} \right\} \vdash x \mathcal{R} z ?$$

$$x - y \in n\mathbb{Z}$$

$$\underline{y - z \in n\mathbb{Z}}$$

$$\underline{x - z \in n\mathbb{Z}}$$

somme de 2 éléments de $n\mathbb{Z}$.

oui, $x \mathcal{R} z$.

Donc \mathcal{R} est relation d'équivalence; elle permet de définir des classes

Une classe = $\{y; y \in \mathbb{Z} / x \mathcal{R} y, x \text{ étant l'élément choisi pour reconnaître la classe}\}$

Tous les éléments de \mathbb{Z} peuvent être ainsi classés et l'ensemble des classes ou ensemble-quotient de \mathbb{Z} par la relation \mathcal{R} que l'on note $\mathbb{Z}/n\mathbb{Z}$ va être étudié:

$$\text{ex: } n = 3$$

Pour placer tout entier relatif dans une classe et une seule, utilisons le théorème suivant:

$x - y \in n\mathbb{Z} \implies x$ et y donnent le même reste dans la division par n .

En effet :

$$* x = nq + r \quad 0 \leq r < n$$

$$y = nq' + r$$

$$x - y = \underbrace{n}_{\in \mathbb{N}^*} \underbrace{(q - q')}_{\in \mathbb{Z}} \quad \text{car } (q, q') \in \mathbb{Z}^2$$

$$* x - y \in n\mathbb{Z}$$

$$\text{On divise } x \text{ par } n: \quad \underline{x = nq + r} \quad 0 \leq r < n$$

$$\text{or } x - y = nq'$$

$$\begin{aligned} y &= x - nq' = (nq + r) - nq' \\ &= n \underbrace{(q - q')}_{\in \mathbb{Z}} + r \end{aligned}$$

$$\underline{y = nr + r} \quad 0 \leq r < n$$

$r =$ reste de y par n .

Revenons à la recherche des classes de $\mathbb{Z}/3\mathbb{Z}$:

$$1^\circ / r = 0, \quad x = \begin{cases} 3 \\ nq \end{cases} \quad \forall q \in \mathbb{Z}$$

$$2^\circ / r = 1, \quad x = nq + 1$$

$$3^\circ / r = 2, \quad x = nq + 2$$

Tous les $x \in \mathbb{Z}$ ont été classés.

$$\mathbb{Z}/3\mathbb{Z} = \{ \text{cl de } 0 ; \text{cl de } 1 ; \text{cl de } 2 \}$$

$$\mathbb{Z}/3\mathbb{Z} = \{ \bar{0} ; \bar{1} ; \bar{2} \}$$

$$\mathbb{Z}/n\mathbb{Z} = \{ \underbrace{\bar{0} ; \bar{1} ; \dots ; \bar{n-1}}_{n \text{ classes}} \}$$

$$\text{Si } n = 5, \quad \left. \begin{array}{l} -37 \in \bar{3} \\ -57 \in \bar{3} \end{array} \right\} \bar{3} \in \mathbb{Z}/5\mathbb{Z}$$

$$\bar{3} \subset \mathbb{Z}$$

$$20 \in \bar{0}$$

On dit que -37 et -57 sont congrus modulo 5

$$20 \text{ et } -75 \quad " \quad " \quad "$$

On écrit :

$$-37 \equiv -57 \quad [5]$$

$$+20 \equiv -75 \quad (\text{mod. } 5)$$

$$45 \equiv 0 \quad [5]$$

8 10

Compatibilité de + et de \mathbb{Q}

de x et de \mathbb{Q}

$$1^\circ \quad x \equiv x' \quad [n]$$

$$y \equiv y' \quad [n]$$

$$x+y \equiv x'+y' \quad [n] \quad ?$$

$$\text{oui car } x-x' \in n\mathbb{Z} \quad , \quad y-y' \in n\mathbb{Z}$$

$$(x - x') + (y - y') \in n\mathbb{Z} \quad n\mathbb{Z} \text{ est un sous-groupe}$$

$$(x + y) - (x' + y') \in n\mathbb{Z}$$

$$\underline{x + y \equiv x' + y' [n]}$$

$$x' \in \dot{x}, \quad y' \in \dot{y}$$

$$x' + y' \in \overline{x + y}$$

$$2/ \quad x \times y \equiv x' \times y' [n]$$

$$\text{Or, } x = x' + n k \quad k \in \mathbb{Z}$$

$$y = y' + n k' \quad k' \in \mathbb{Z}$$

$$x y = x' y' + n (\underbrace{k y' + k' x' + n k k'}_{K \in \mathbb{Z}})$$

$$x y = x' y' + n K$$

$$\underline{x y \equiv x' y' [n]}$$

$$x' \in \dot{x}, \quad y' \in \dot{y}$$

$$x' y' \in \overline{x y}$$

Génération + etc. x dans $\mathbb{Z}/n\mathbb{Z}$

Définition

$$\dot{x} + \dot{y} = \overline{x + y}$$

$$\dot{x} \dot{y} = \overline{x \times y}$$

Homomorphisme canonique de \mathbb{Z} sur $\mathbb{Z}/n\mathbb{Z}$

$$f: \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

$$x \longmapsto \bar{x} = f(x)$$

$$y \longmapsto \bar{y} = f(y)$$

$$\underbrace{x+y}_z \longmapsto \underbrace{\bar{x} + \bar{y}}_{\bar{z}} = f(z)$$

$$f(x+y) = f(x) + f(y)$$

f est un homomorphisme de $(\mathbb{Z}, +)$ dans $(\mathbb{Z}/n\mathbb{Z}, +)$

De plus f est surjective:

$$\forall \bar{x} \in \mathbb{Z}/n\mathbb{Z}, \exists x, x \in \mathbb{Z} / f(x) = \bar{x}$$

f = homomorphisme surjectif.

De même :

$$f: \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

$$x \longmapsto \bar{x} = f(x)$$

$$y \longmapsto \bar{y} = f(y)$$

$$x \times y \longmapsto \underbrace{\bar{x}}_{f(x)} \times \underbrace{\bar{y}}_{f(y)} = f(x \times y)$$

$$\varphi(xy) = \varphi(x) \cdot \varphi(y)$$

φ est un homomorphisme surjectif de $(\mathbb{Z}, +)$ sur $(\mathbb{Z}/n\mathbb{Z}, +)$

Structure de $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

9 10

1°/ $(\mathbb{Z}/n\mathbb{Z}, +)$ groupe commutatif.

* $\forall (x, y, z) \in (\mathbb{Z}/n\mathbb{Z})^3$, a-t-on :

$$(x + y) + z = x + (y + z) \quad ?$$

$$\overline{x+y} + \overline{z} = \overline{x} + \overline{y+z} \quad ?$$

$$\overline{(x+y)+z} = \overline{x+(y+z)} \quad ?$$

$+$ est associative dans \mathbb{Z} , donc la réponse est oui.

* $\exists \dot{0} \in \mathbb{Z}/n\mathbb{Z} \mid \forall x \in \mathbb{Z}/n\mathbb{Z}$,

$$\underbrace{\overline{x} + \dot{0}}_{x+0} = \underbrace{\dot{0} + \overline{x}}_{0+x} = \overline{x}$$

(0 neutre dans $(\mathbb{Z}, +)$)

* $\forall x \in \mathbb{Z}/n\mathbb{Z}$, $\exists \overline{-x} \in \mathbb{Z}/n\mathbb{Z}$

$$\underbrace{\overline{x} + \overline{-x}}_{x+(-x)} = \overline{-x} + \overline{x} = \dot{0}$$

* $\forall x \in \mathbb{Z}/n\mathbb{Z}$, $\forall y \in \mathbb{Z}/n\mathbb{Z}$

$$x + y = y + x$$

$$\overline{x+y} = \overline{y+x}$$

oui.

$$2) (\mathbb{Z}/n\mathbb{Z}, +, \times)$$

$$* \forall (x, y, z) \in (\mathbb{Z}/n\mathbb{Z})^3$$

$$(\overline{x \times y}) \times \overline{z} = \overline{x \times (y \times z)} \quad ?$$

$$\overline{xy} \times \overline{z} = \overline{x \times yz}$$

$$\overline{(xy) \times z} = \overline{x(yz)}$$

$$\overline{xyz} = \overline{xyz} \quad \text{oui.}$$

$$* (\overline{x+y}) \times \overline{z} = \overline{x \times z} + \overline{y \times z} \quad ?$$

distributivité à droite.

$$\overline{x+y} \times \overline{z} = \overline{xz} + \overline{yz}$$

$$\overline{(x+y) \times z} = \overline{xz + yz}$$

oui

$$* \forall x \in \mathbb{Z}/n\mathbb{Z} ; \quad x \times 1 = 1 \times x = x$$

$$\overline{x \cdot 1} = \overline{1 \cdot x} = \overline{x}$$

$$* \overline{x \times y} = \overline{y \times x} \quad ?$$

$$\overline{xy} = \overline{yx}, \quad \text{oui.}$$

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$: anneau commutatif unitaire.

De plus, il se peut que $\forall x \in \mathbb{Z}/n\mathbb{Z} - \{0\}$, il existe $x' \in (\mathbb{Z}/n\mathbb{Z})^* / x x' = 1$

x' : classe inverse de x .

Mais ce n'est pas général.

Si cela est vrai, alors $(\mathbb{Z}/n\mathbb{Z})^*$ est un groupe multiplicatif

$n=5$							$n=6$						
\bar{x}	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$		\bar{x}	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$		$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$		$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$		$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$		$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$		$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
							$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$(\mathbb{Z}/5\mathbb{Z}, +, \cdot) = \text{corps commutatif.}$

$(\mathbb{Z}/6\mathbb{Z}, +, \cdot) = \text{anneau unitaire commutatif.}$

Remarque.

$(\mathbb{Z}/5\mathbb{Z}, +, \cdot) = \text{anneau int\`egre:}$

$$x \cdot y = 0 \iff x = 0 \text{ ou } y = 0$$

(voir table).

2°/ Toute classe, sauf $\bar{0}$, est inversible.

$$\forall \underline{x \neq 0}, \exists x' \quad / \quad x \times x' = 1$$

démonstration
général

$$\text{Or} \quad \underbrace{x' \times x}_{=1} \times y = x' \times 0$$

$$1 \times y = 0 \quad \vdash \quad \underline{y=0}$$

4 10

5

Rappel : $a|b$ - PGCD

$$a|b \mapsto b \cdot \mathbb{Z} \subset a \cdot \mathbb{Z}$$

1) $a|a$ oui (Réflexivité)2) $a|b$ et $b|a \mapsto a=b$ (Antisymétrie)3) $a|b$ et $b|c \mapsto a|c$ (Transitivité).La relation $|$ (se lit 'divise') est relation d'ordre.

L'inclusion aussi :

$$* A \subset B, \forall A \in E$$

$$* A \subset B \text{ et } B \subset A \mapsto A=B$$

$$* A \subset B \text{ et } B \subset C \mapsto A \subset C$$

Remarque

 $|$ est d'ordre dans \mathbb{N} mais, dans \mathbb{Z} , l'antisymétrie n'est pas réalisée :

$$1|-1 \text{ et } -1|1 \text{ et pourtant } 1 \neq -1$$

De plus, les 2 relations sont d'ordre partiel.

Donne de deux idéaux

$$(a) = a \cdot \mathbb{Z}, a \neq 0$$

$$(b) = b \cdot \mathbb{Z}, b \neq 0$$

$$\mathcal{J} \subset \mathbb{Z} \quad / \quad \mathcal{J} = \{x, x \in \mathbb{Z} \mid \exists (u, v) \in \mathbb{Z}^2 : x = au + bv\}$$

$$1^\circ \mathcal{J} \neq \emptyset \quad (\text{voir } 0, a, b \in \mathcal{J})$$

$$\forall x \in \mathcal{J}, \forall y \in \mathcal{J}, \quad x - y \in \mathcal{J}?$$

$$\begin{cases} x = au + bv \\ y = au' + bv' \end{cases}$$

$$x - y = a \underbrace{(u - u')}_{\in \mathbb{Z}} + b \underbrace{(v - v')}_{\in \mathbb{Z}} \in \mathcal{J}$$

$(\mathcal{J}, +)$ sous-groupe de \mathbb{Z} .

$$2^\circ \forall x \in \mathcal{J}, \forall z \in \mathbb{Z}, \quad x \cdot z \in \mathcal{J}?$$

$$(au + bv)z = a \underbrace{(uz)}_{\in \mathbb{Z}} + b \underbrace{(vz)}_{\in \mathbb{Z}} \in \mathcal{J}$$

\mathcal{J} est partie "multiplicativement fermée" de \mathbb{Z}

\mathcal{J} = idéal de \mathbb{Z} .

$$\mathcal{J} = (a) \oplus (b)$$

$$\exists \delta > 0 \text{ si et seulement si } \mathcal{J} \neq \{0\}$$

$$\text{Gr, } a \in \mathcal{J} \text{ et } a \neq 0$$

$$\text{Donc } \mathcal{J} \neq \{0\}, \text{ donc } \delta > 0 \text{ et}$$

$$\mathcal{J} = \delta \mathbb{Z}$$

Comparaison de δ et a .

$$a = a \cdot 1 + b \cdot 0 \in \mathcal{I}$$

$$\underline{a} = \underline{\delta} q \quad \vdash \quad \boxed{\delta \mid a}$$

$$(a) \subset (\delta) \quad (\text{ou } a \in \delta \mathbb{Z} \text{ ou } (a) \subset \mathcal{I})$$

De même $(b) \subset (\delta)$

$$\boxed{\delta \mid b}$$

De plus, $\delta \in \delta \mathbb{Z}$

$$\exists (u_0, v_0) \in \mathbb{Z}^2 \quad / \quad \boxed{\delta = \underline{a} u_0 + \underline{b} v_0}$$

Conséquence

Tout $d \in \mathbb{Z}$ tel que $d \mid \delta$ est tel que $d \mid a$

De même $d \mid b$.

Tout diviseur de δ divise a et b

Inversement, tout d' qui divise a et b permet d'

$$\text{écrire : } a = d' q_0, \quad q_0 \in \mathbb{Z}$$

$$b = d' q_1, \quad q_1 \in \mathbb{Z}$$

$$\text{et } \delta = d' q_0 u_0 + d' q_1 v_0$$

$$\delta = d' \underbrace{(q_0 u_0 + q_1 v_0)}_{\in \mathbb{Z}} \quad \vdash \quad d' \mid \delta$$

Tout diviseur commun à a et b divise δ

$$d \text{ divise } a \text{ et } b \quad \longmapsto \quad d \text{ divise } \delta$$

$$d \in \mathbb{Z}$$

Remarque : $a \in \mathbb{N}^*$, $b \in \mathbb{N}^*$ et $\delta \in \mathbb{N}^*$

Dans le cas où $\delta = 1$, on dit que a et b sont premiers entre eux :

$$1 = a u_0 + b v_0$$

"Si" a et b sont premiers entre eux" équivaut à :

$$\exists (u_0, v_0) \in \mathbb{Z}^2 \mid a u_0 + b v_0 = 1.$$

21.10

L'entier naturel δ évoqué dans ce qui précède n'est autre que le plus grand des diviseurs communs à a et b (a et b entiers relatifs ; souvent naturels)

$$\delta = \text{PGCD de } a \text{ et } b$$

$$\delta = \Delta(a, b) = a \wedge b$$

Si $\Delta(a, b) = 1$, a et b sont dits premiers entre eux sont $+1$ et -1 .

$a u_0 + b v_0 = 1$ est dite "égalité de Bézout".

$$\text{ex: } a = +6, b = -7$$

$$\exists u_0 = 13, v_0 = 11 \mid 6 \times 13 + (-7) \times 11 =$$

En effet $78 - 77 = +1$

$$\Delta(6, -7) = +1$$

Propriétés du PGCD de a et b

$$1^\circ \quad \delta = \Delta(a, b) \quad , (a, b) \in \mathbb{Z}^{* \times 2}$$

$$\delta' = \Delta(ca, cb) \quad , c \in \mathbb{Z}^*$$

$$\delta' \mathbb{Z} = (\delta') = \left\{ x, x \in \mathbb{Z} \mid \exists (u, v) \in \mathbb{Z}^2, x = ca \cdot u + cb \cdot v \right\}$$

$$\text{Or, } x = c(au + bv)$$

$au + bv$ est élément de (δ) , et inversement, tout élément de (δ) est de cette forme. De plus, tout

$x \in \delta' \mathbb{Z}$ est multiple de c . Donc, le plus petit entier positif de $\delta' \mathbb{Z}$ est $|c| \cdot \delta$; or, c'est δ' par définition :

$$\delta' = |c| \cdot \delta \quad (1)$$

$$2^\circ \quad \delta = \Delta(a, b)$$

Soit d un diviseur commun à a et b .

$$a = d a' \quad , \quad b = d b' \quad , \quad (a', b') \in \mathbb{Z}^{* \times 2}$$

$$\delta' = \Delta(a', b')$$

$$\delta = \Delta(a'd, b'd) = \Delta(a, b)$$

$$\text{donc : (cf } 1^\circ) \quad \delta = \delta' \cdot |d| \quad \text{donc :}$$

$$\delta' = \frac{\delta}{|d|} \quad (2)$$

Conséquence

Preons $d = \delta = \Delta(a, b)$

$$\Delta\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{\delta}{\delta} = 1$$

$$\Delta\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = 1 \iff \frac{a}{\delta} \text{ et } \frac{b}{\delta} \text{ premiers entre eux}$$

Inversement, soit $d \in \mathbb{Z}^*$ un diviseur commun

$$a \text{ et } b : \frac{a}{d} = a' \in \mathbb{Z}^*, \frac{b}{d} = b' \in \mathbb{Z}^*$$

$$\text{Si } \Delta(a', b') = 1, \text{ c'est que } \frac{\Delta(a, b)}{|d|} = 1$$

$$d = \pm \Delta(a, b)$$

Ces 2 propriétés réciproques l'une de l'autre forment

un critère de PGCD:

Parmi tous les diviseurs communs de a et b , le PGCD est celui qui vérifie : "Les quotients, entiers de a et b par ce diviseur, sont premiers entre eux"

$$3^\circ / \Delta(a, b) = 1 \text{ et } \Delta(a, c) = 1$$

a est donc premier avec b et c par hypothèse.

$$\exists (u_0, v_0) \in \mathbb{Z}^2 / a u_0 + b v_0 = 1$$

$$\underline{a} c u_0 + \underline{b} c v_0 = c$$

Tout diviseur d commun à a et $b c$ divise $a c u_0$, $b c v_0$, donc leur somme, donc c (et inversement 1).

$$\text{Or, } \Delta(a, c) = 1 \implies d = \pm 1 \implies \text{la seule diviseur commun est } 1$$

$$\Delta(a, b c) = 1$$

$$\Delta(a, b) = 1 \text{ et } \Delta(a, c) = 1 \implies \Delta(a, b c) = 1 \quad (3)$$

a , premier avec b et c , est premier avec le produit $b c$

4° / Théorème de Gauss.

$$\text{hyp. } \begin{cases} a | b c, & a \in \mathbb{Z}^*, (b, c) \in \mathbb{Z}^{*2} \\ \Delta(a, c) = 1 \end{cases}$$

$$\exists (u_0, v_0) \in \mathbb{Z}^2 / a u_0 + c v_0 = 1$$

$$\underline{b a} u_0 + \underline{b c} v_0 = b$$

\underline{a} divisant $b a u_0$ et $b c v_0$, divise leur somme, donc divise b

Remarque - conséquence du théorème de Gauss

$$\Delta(a, c) = 1 \implies \begin{matrix} a | c \text{ et } b | c \\ \hline a | c \text{ et } b | c \end{matrix} \implies a b | c$$

a divisant b.c, et premier avec c, divise
alors nécessairement b. (4)

Application

Résoudre en nombres entiers, l'équation :

$$6x - 7y = 1, \quad (x, y) \in \mathbb{Z}^2$$

6 et 7 sont premiers entre eux. L'égalité de Bezout
est vérifiée pour un couple au moins (x, y)

$$\text{car : } x = -1, y = -1$$

$$\begin{cases} 6x - 7y = 1 \\ 6(-1) - 7(-1) = 1 \end{cases}$$

$$6(x+1) - 7(y+1) = 0$$

$$6(x+1) = 7(y+1)$$

6 divise le 1^{er} membre (voir $x+1 \in \mathbb{Z}$). Donc

6 divise le 2nd membre. Or, 6 est premier avec 7

donc (théorème de Gauss) 6 divise $y+1$

$$y+1 = 6q, \quad q \in \mathbb{Z}$$

De $6(x+1) = 7(y+1)$ on tire :

$$6(x+1) = 7 \cdot 6q$$

$$x+1 = 7q$$

$$\begin{cases} x = 7q - 1 \\ y = 6q - 1 \end{cases} \quad q \in \mathbb{Z}$$

$$x \in \{ \dots, -15, -8, -1, 6, 13, 20, \dots \}$$

$$y \in \{ \dots, -13, -7, -1, 5, 11, 17, \dots \}$$

22.10

recherche pratique de $\Delta(a, b)$

$a \in \mathbb{N}^*$, $b \in \mathbb{N}^*$ (cela n'enlève rien à la généralité de la méthode). ($a > b$).

Sinon, on opère avec $|a|$ et $|b|$.

1°) $a = bq$, tout diviseur de b divise a .

$$\Delta(a, b) = b$$

$$2^\circ) a = bq + r \quad 0 \leq r < b$$

(a, $\Delta(a, b) = \Delta(b, r)$ car, r).

α) tout d qui divise a et b divise a , bq , $a - bq$, donc r ; donc b et r .

β) tout d qui divise b et r divise bq et r , a ; donc a et b .

γ) Les éléments les plus grands des 2 listes de diviseurs communs (listes identiques) coïncident.

On reprend le couple (b, r) et on fait une nouvelle division: $b = r q_1 + r_1$, $0 < r_1 < r$.

$$\Delta(b, r) = \Delta(r, r_1)$$

$$r = r_1 q_2 + r_2, \quad 0 < r_2 < r_1$$

$$r_{n-2} = r_{n-1} q_n + \boxed{r_n}, \quad 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n q_{n+1} + 0.$$

Nécessairement, l'algorithme (succession d'opérations répétées) se termine car les restes trouvés, entiers naturels, sont de plus en plus petits.

Il existe un dernier reste non nul. La dernière

ligne montre: $\Delta(r_{n-1}, r_n) = r_n$

$$\text{Or, } \Delta(r_{n-1}, r_n) = \Delta(r_{n-2}, r_{n-1}) = \dots$$

$$= \Delta(r_1, r_2)$$

$$= \Delta(r, r_1) = \Delta(b, r)$$

$$= \Delta(a, b)$$

$$\boxed{\Delta(a, b) = \underbrace{\Delta(b, r)}_{r_n}}$$

Exemple

$$a = 2375, b = 75$$

$$2375 = 75 \times 31 + 50 \quad 50 < 75$$

$$75 = 50 \times 1 + \underline{25} \quad 25 < 50$$

$$50 \cancel{25} = \underline{25} \times 2 + 0$$

$$a_n = 25$$

$$\Delta(2375, 75) = 25$$

Application

$$\text{Résoudre dans } \mathbb{Z}^2 \quad 437x - 241y = 1$$

$$437 = 241 \times 1 + 196$$

$$241 = 196 \times 1 + 45$$

$$196 = 45 \times 4 + 16$$

$$45 = 16 \times 2 + 13$$

$$16 = 13 \times 1 + 3$$

$$13 = 3 \times 4 + \underline{1}$$

$$3 = \underline{1} \times 3 + 0$$

$$\Delta(437, 241) = 1$$

437 et 241 sont premiers entre eux.

On exprime les restes successifs uniquement à l'aide

de 437 et de 241.

$$\underline{196 = 437 - 241}$$

$$45 = 241 - 196 = 241 - (437 - 241)$$

$$\underline{45 = 2 \cdot 241 - 437}$$

$$16 = (437 - 241) - 8 \cdot 45 = 437 - 241 - 8(2 \cdot 241 - 437)$$

$$\underline{16 = 5 \cdot 437 - 9 \cdot 241}$$

$$13 = 2 \cdot 241 - 437 - 2(5 \cdot 437 - 9 \cdot 241)$$

$$\underline{13 = 20 \cdot 241 - 11 \cdot 437}$$

$$3 = 5 \cdot 437 - 9 \cdot 241 - 20 \cdot 241 + 11 \cdot 437$$

$$\underline{3 = 16 \cdot 437 - 29 \cdot 241}$$

$$1 = 20 \cdot 241 - 11 \cdot 437 - 4(16 \cdot 437 - 29 \cdot 241)$$

$$\underline{1 = -75 \cdot 437 + 136 \cdot 241}$$

$$\exists (x_0, y_0) = (-75, -136)$$

Alors.

$$\begin{cases} 437x - 241y = 1 & (1) \\ 437(-75) - 241(-136) = 0 \end{cases}$$

$$437(x+75) = 241(y+136) \quad (2)$$

Théorème de Gauss. $y+136 = 437k$

$\forall k \in \mathbb{Z}$. On remplace dans (2):

$$x+75 = 241k$$

$$\begin{cases} x = 241k - 75 \\ y = 437k - 136 \end{cases} \quad \forall k \in \mathbb{Z}$$

$$\begin{cases} x \equiv -75 \ [241] \\ y \equiv -136 \ [437] \end{cases}$$

5.121

Diviseur commun à plusieurs entiers relatifs

$$1^\circ \quad \{a_1, a_2, a_3, \dots, a_k\} \quad (a_i)_{i \in [1, k] \cap \mathbb{N}} \neq \emptyset$$

$$(a_1) = a_1 \mathbb{Z} \quad \text{ou} \quad (a_1) = -a_1 \mathbb{Z}$$

$$(a_k) = a_k \mathbb{Z} \quad \text{ou} \quad (a_k) = -a_k \mathbb{Z}$$

$$A = (a_1) + (a_2) + \dots + (a_k) = \left\{ x \in \mathbb{Z}, \exists u_1, \dots, u_k \in \mathbb{Z} / \right.$$

$$\left. x = a_1 u_1 + \dots + a_k u_k \right\}$$

A est un idéal de \mathbb{Z}

$$\alpha) \quad A \neq \emptyset \quad (\exists a_1 \in A)$$

$$\beta) \quad (A, +) \text{ sous-groupe de } \mathbb{Z}$$

$$\gamma) \quad \forall x \in A, \forall y \in \mathbb{Z}, x + y \in A$$

$A \neq \{0\}$, sinon, c'est qu'on se serait donné tous les

a_i nuls. $\exists! \delta > 0$, δ minimum et $\delta \in A$

$$\text{Alors} \quad A = \delta \mathbb{Z}$$

$$* \quad a_i \in A \quad \vdash \quad \exists q \in \mathbb{Z} / a_i = \delta q$$

δ divise tous les a_i : $\delta \mid a_i$

$$* \quad \delta \in A \mid \delta = a_1 v_1 + a_2 v_2 + \dots + a_k v_k \\ \exists (v_1, \dots, v_k) \in \mathbb{Z}^k$$

$\forall d \in \mathbb{Z} \mid d \mid a_i, \forall i \in [1, k] \cap \mathbb{N}$, divise δ

Donc $\delta = \text{PGCD}(a_1, a_2, \dots, a_k)$

Remarque

Si $\delta = 1$, $\exists (u_1, u_2, \dots, u_k) \in \mathbb{Z}$

$$1 = a_1 u_1 + \dots + a_k u_k$$

Les a_i sont dits "premiers entre eux dans leur ensemble"

3.11

6

PPCM de 2 entiers relatifs non nuls a et b

$$(a) = \{x, x \in \mathbb{Z}; \exists k \in \mathbb{Z} : x = ka\} = a\mathbb{Z}$$

$$(b) = \{x, x \in \mathbb{Z} / \exists k \in \mathbb{Z} : x = kb\} = b\mathbb{Z}$$

$$J = (a) \cap (b) = \text{idéal ?}$$

* $J = (a) \cap (b)$ est-il un sous-groupe de \mathbb{Z}

En effet, $J \neq \emptyset$: voir $0 = 0 \cdot \underline{a} = 0 \cdot \underline{b}$

$$a \cdot b = b \cdot a = a \cdot \underline{b}$$

et : $\forall x \in J, \forall y \in J, x + (-y) \in J$?

$$x \in J \mapsto x = ka = k'b, (k, k') \in \mathbb{Z}^2$$

$$y \in J \mapsto y = qa = q'b, (q, q') \in \mathbb{Z}^2$$

$$x - y \in \underbrace{(k - q)}_{\in \mathbb{Z}} a = \underbrace{(k' - q')}_{\in \mathbb{Z}} b$$

$$x - y = Qa = Q'b, (Q, Q') \in \mathbb{Z}^2$$

$$\underline{x - y \in J}$$

* On a vu que tout sous-groupe de \mathbb{Z} est de la forme $n\mathbb{Z}$, $n \in \mathbb{N}$, donc est un idéal de \mathbb{Z} .
Ici, c'est le cas

$$J = \mu \mathbb{Z} = (\mu)$$

μ étant l'entier naturel le plus petit de J .

$$\boxed{\mu = \text{PPCM de } a \text{ et } b, \mu > 0}$$

ex: $a = 45$ et $b = 10$

$$\mu = 90 = \underbrace{2}_{k} \times 45 = \underbrace{9}_{k'} \times 10$$

Propriétés du PPCM

1°/

$$\mu = M(a, b) = \text{PPCM de } (a, b) = a \vee b = a \vee b$$

$$\mu' = M(ka, kb), k \in \mathbb{Z}$$

$$\forall m' \in (\mu'), m' = ka p = kb q \quad (p, q) \in \mathbb{Z}$$

$$m' = kp a = kq b \in (\mu)$$

$$m' = k \mu, k \in \mathbb{Z}$$

Revenons à :

$$m' = \underbrace{k(p a)}_{h_1 \mu} = \underbrace{k(q b)}_{h_1 \mu}$$

$$m' = k \cdot h_1 \cdot \mu$$

$$m' = k \cdot h_1 (k \cdot \mu)$$

m' est un multiple de $k \mu$.

$$m' \in (k\mu) \quad \text{donc} \quad (\mu') \subset (k\mu)$$

Inversement, soit $m'' \in (k\mu)$

$$m'' = k(k\mu) = k(k\mu)$$

$$m'' = k(k\mu)$$

$$m'' = k \cdot pa = k \cdot qb$$

$m'' = p(ka) = q(kb) \vdash m'' = \text{multiple commun}$
 $\in ka \text{ et } kb$. Donc $m'' \in (\mu')$

$$(k\mu) \subset (\mu')$$

∠

$$(\mu') = (k\mu) \vdash \mu' = |k|\mu$$

3°/ Conséquence

$$\mu = M(a, b)$$

$$a = d a' \quad , \quad d \in \mathbb{Z}$$

$$b = d b' \quad d = \text{diviseur commun à } a \text{ et } b.$$

$$\mu' = M(a', b')$$

$$|d|\mu' = M(\underbrace{da'}_a, \underbrace{db'}_b)$$

$$\mu = |d|\mu'$$

$$\mu' = \frac{\mu}{|d|}$$

$$M\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{M(a, b)}{|d|}$$

3) Une relation entre a, b, δ et μ .

$$\begin{cases} \Delta(k a, k b) = |k| \Delta(a, b) & \text{(rappel)} & (1) \\ M(k a, k b) = |k| M(a, b) & & (2) \end{cases}$$

α) $|k| = M(a, b) = \mu$ dans la 1^{re} égalité. ($k = \mu$)

(1) devient : $\mu \cdot \delta = \Delta(\mu a, \mu b)$

$$\mu a = a \mu = a \cdot M(a, b) = M(a^2, \underline{a b})$$

$$\mu b = b \mu = b \cdot M(a, b) = M(\underline{a b}, b^2)$$

$(a b)$ divise donc $\Delta(\mu a, \mu b)$ donc $\mu \delta$
 $a b$ divise $\mu \delta$

$$\beta) |k| = \Delta(a, b) = \delta = k$$

(2) devient : $\delta \mu = M(a \delta, b \delta)$

$$a \delta = a \Delta(a, b) = \Delta(a^2, \underline{a b})$$

$$b \delta = b \Delta(a, b) = \Delta(\underline{a b}, b^2)$$

(a, b) est donc multiple de $\mu \delta$

Résumé: $a \delta \mid \mu \delta$

$$\mu \delta \mid a \delta$$

Donc $\mu \delta = |a \delta|$

$$\mu \delta = |a \delta|$$

Remarque 1: La relation \mid est relation d'ordre dans \mathbb{N} , mais pas dans \mathbb{Z} .

Remarque 2: Si $a > 0$ et $b < 0$, $b = -b_1$ avec $b_1 > 0$. $|a b| = a b_1$

On se place dans le cas où a et b sont tous deux positifs $|a b| = |a b_1| = \mu \delta$

(même μ et même δ pour les couples (a, b) et (a, b_1))

$$a > 0, b > 0$$

$$\begin{cases} a = \delta a' \\ b = \delta b' \end{cases} \quad \text{et} \quad \Delta(a', b') = 1$$

La relation $a b = \mu \delta$ devient

$$\delta a' \cdot \delta b' = \mu \delta$$

$$\delta a' b' = \mu$$

$$a \in a' = a \vdash$$

$$\text{et } \delta b' = b \vdash$$

$$\mu = a b'$$

$$\mu = a' b$$

$$\mu\delta = a\delta$$

$$\text{si } a\delta > 0$$

$$\mu = \delta a' \delta' = a\delta' = \delta a'$$

$$\Delta(a', \delta') = 1$$

Application - exercice

$$1) \begin{cases} M(a, \delta) = 60 \\ a = 12 \end{cases}$$

trouver δ

$\alpha)$ Supposons $\delta > 0$.

$$60 - \delta = 12 \cdot \delta$$

$$5\delta = \delta \quad \leftarrow \delta = \text{multiple de } 5$$

et δ divise 60

$$\delta = 5, 10, 15, 20, 30, \text{ ou } 60$$

Il existe 6 solutions.

$\beta)$ Supposons $\delta < 0$.

$$\delta = -5, -10, -15, -20, -30, \text{ ou } -60$$

$$\begin{cases} \delta = 36 ; \mu = 756 \\ \delta = \Delta(a, b) ; \mu = M(a, b) \end{cases}$$

Trouver (a, b) ?

Posez $|a| = \alpha ; |b| = \beta$

$$\alpha \beta = \mu \delta$$

$$\alpha \beta = 756 \times 36$$

$$\begin{cases} \alpha = \delta \alpha' \\ \beta = \delta \beta' \end{cases} \text{ avec } \Delta(\alpha', \beta') = 1$$

$$\delta^2 \alpha' \beta' = 756 \times 36 \quad (\alpha', \beta') \in \mathbb{N}^2$$

$$756 = 36 \times 21 \quad (\text{énoncé favorable})$$

Donc $36 \times 36 \times \alpha' \beta' = 36 \times \cancel{36} \times 21$

$$\begin{cases} \alpha' \beta' = 21 \\ \Delta(\alpha', \beta') = 1 \end{cases}$$

α' et β' sont des diviseurs de 21.

La liste en est ($>$) : 21 ; 7 , 3 ; 1

$$\alpha' = 21 \text{ et } \beta' = 1$$

ou $\alpha' = 7 \text{ et } \beta' = 3$

Si on demande des couples (α', β') , il y en a 4.
Sinon, il y a deux paires.

$$\begin{cases} \alpha = \delta \alpha' = 36 \times 21 \\ \beta = \delta \beta' = 36 \times 1 \end{cases}$$

$$\begin{cases} \alpha = 36 \times 7 \\ \beta = 36 \times 3 \end{cases} \quad \text{vérification : } 36 \cdot 7 \cdot 36 \cdot 3 = 756 \cdot 3$$

\exists 4 couples (α, β)

\exists 16 couples (a, b) : signes associés $\begin{cases} + & + \\ - & - \\ + & - \\ - & + \end{cases}$

3/ On donne $d = \mu - \delta = 18$ (1)

$$\mu \delta = \alpha \beta = |\alpha| \times |\beta|$$

$$\mu \delta = \alpha \beta = \delta \alpha' \cdot \delta \beta'$$

$$\mu = \delta \alpha' \beta'$$

(1) : $d = \delta \alpha' \beta' - 1 \delta$

$$18 = \underbrace{\delta}_{\in \mathbb{N}} (\underbrace{\alpha' \beta' - 1}_{\in \mathbb{N}})$$

$$\Delta(\alpha', \beta') = 1$$

δ est un diviseur positif de 18.

$$18, 9, 6, 3, 2, -1$$

donc

$$\alpha' \beta' - 1 = -1 \text{ ou } 2 \text{ ou } 3 \text{ ou } 6 \text{ ou } 9 \text{ ou } 18$$

$$\{\alpha'\beta' = 2, 3, 4, 7, 10, \text{ ou } 19$$

$$\Delta(\alpha', \beta') = 1; \vdash \alpha' \beta' = 2 \quad \alpha' = 1 \text{ et } \beta' = 2$$

$$\alpha'\beta' = 2 \vdash \{\alpha', \beta'\} = \{1, 2\} \quad (\text{ou inversément})$$

$$\alpha'\beta' = 3 \vdash \{\alpha', \beta'\} = \{-1, 3\}$$

$$\alpha'\beta' = 4 \vdash \{\alpha', \beta'\} = \{-1, 4\}$$

$$\alpha'\beta' = 7 \vdash \{\alpha', \beta'\} = \{1, 7\}$$

$$\alpha'\beta' = 10 \vdash \{\alpha', \beta'\} = \{-1, 10\} \text{ ou } \{2, 5\}$$

$$\alpha'\beta' = 19 \vdash \{\alpha', \beta'\} = \{1, 19\}$$

$$\{\alpha, \beta\} = \{-18, 36\} \quad \text{car } \delta = 18$$

$$\{\alpha, \beta\} = \{9, \frac{27}{2}\} \quad \text{car } \delta = 9$$

$$\{\alpha, \beta\} = \{6, 24\} \quad \text{car } \delta = 6$$

etc ...

Nombres premiers

p premier a 4 diviseurs : $\{\underline{1}, -1, \underline{p}, -p\}$

$1 \neq$ nombre premier

2, 3, 7, 11 sont premiers

16 \neq nombre premier

Première propriété

Z

" Tout nombre non premier ^($\neq 1$) admet au moins un diviseur premier : c'est le plus petit des diviseurs du nombre donné, du moins dans $\mathbb{N} - \{1\}$

ex: 42 a pour diviseurs :

42, -42, 21, -21, 7, -7, 6, -6, 3, -3, 1, -1, 14, -14, 2, -2.

143 a pour diviseurs : 143, 13, 11, 1, -1, -11, -13, -143, -13, -11.

$$n = \underline{d} \cdot d'$$

$$d \leq d'$$

ex $49 = \underline{7} \times 7$ ou : $143 = \underline{11} \times 13$

$d \leq d'$ (d = le diviseur premier signalé ci-dessus.)

$$d^2 \leq dd'$$

$$d^2 \leq n$$

Donc n non premier différent de 1 admet $d \neq 1$,
et d premier tel que $d^2 \leq n$.

C'est la contraposée de cette propriété qui est utile pratiquement :

Pour chercher si un nombre n est, ou non, premier, on effectue les divisions successives de n par les entiers naturels premiers à partir du plus petit et dans l'ordre croissant. De 2 choses l'une.

* ou bien une division donne un reste nul ; n n'est pas premier

* ou bien aucune des divisions par les $d / d^2 \leq n$ n'a donné de reste nul. On conclut que n est premier.

Le critère d'arrêt dans la liste des diviseurs essayés est $d^2 > n$ d est le diviseur essayé.

Il y en a un plus simple

pour 491

exemple : $491 = \textcircled{19} \times \underline{\underline{25}} + 16$
 $491 = \textcircled{23} \times \underline{\underline{21}} + 8$

$$19^2 = 361, \quad 23^2 = 529$$

Quand le quotient devient inférieur au diviseur essayé, alors le carré du diviseur essayé dépasse 491 : alors on peut s'arrêter. 491 est premier.

Plus généralement :
$$\begin{cases} n = \textcircled{p} q + r, & r < p \\ \text{et } q < p \end{cases}$$

donc $pq < p^2$

ou encore $q < p \implies q+1 \leq p$

$$pq + r < pq + p \leq p^2$$

$$pq + r < p^2$$

$$p^2 > n$$

$\underbrace{q < p} \implies p^2 > n$

critère suffisant d'arrêt

l'ensemble des nombres premiers est illimité

Si $\exists p$ premier, on arrive à trouver un p' premier, $p' > p$, donc l'ensemble des nombres premiers n'est pas majoré.

Soit $n = p! + 1$

* ou bien n tombe premier et $\exists n > p$, n premier.

* ou bien $n \neq$ nombre premier et alors n admet au moins 1 diviseur p' premier; mais ce n'est aucun des facteurs premiers composant $p!$ (voir reste égal à 1)

$$n = 2, 3 \dots \textcircled{q} \dots p + 1$$

Donc $p' > p$ et p' premier

nombre premiers et divisibilité ($a, b \in \mathbb{Z}$)

① " p premier est "premier avec" tout a qu'il ne

divise pas:

* $19 \nmid 38$ — 19 n'est pas premier avec 38
 * 19 ne divise pas 37 } 19 premier avec 37 , et avec 64 .
 19 " " 64

② Deux nombres premiers différents ^{en valeurs absolues} sont premiers entre eux.

Soit p_1 et p_2 premiers, si $|p_1| \neq |p_2|$, alors

p_1 et p_2 sont premiers entre eux.

Remarque. 19 et -19 ont 19 pour PGCD
 $\Delta(19, -19) \neq 1$

③ Tout diviseur p premier d'un produit abc ,
divise nécessairement ou a , ou b , ou c .

* Soit p premier diviseur de ab

Il peut diviser a ; sinon, il est premier avec a et
alors le th. de Gauss s'applique :
et p divise b .

* Soit p premier de abc

p peut diviser a ou b ; sinon, il ne divise ni a , ni b
il est donc premier avec les 2; donc premier avec
 ab (théorème du 21.10); puis (th. de Gauss),
 p divise c .

④ Tout diviseur p premier d'un produit abc de
nombres premiers a pour valeur absolue : $|a|$ ou $|b|$ ou $|c|$

et sur l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

$$* n = 0 \quad x \equiv y [0], (x, y) \in \mathbb{Z}^2$$

$$x = y + k \cdot 0 \quad \vdash \quad x = y$$

$$y = x \quad \vdash \quad \bar{x} = \{x\}; \text{ l'ensemble } \mathbb{Z}/0\mathbb{Z} \text{ isomorphe à } \mathbb{Z},$$

anneau.

$$* n = 1 \quad x \equiv y [1]$$

$$x = y + k, k \in \mathbb{Z}$$

$$\exists! 0 \text{ s.t. } x \in 0, y \in 0$$

$$* n \geq 2$$

on cherche les éléments de $\mathbb{Z}/n\mathbb{Z}$ qui sont inversibles.

ex. \bar{x} inversiblessi:

$$\exists x' \in \mathbb{Z}/n\mathbb{Z} \quad / \quad \bar{x} \times \bar{x}' = 1$$

$$\overline{xx'} = 1$$

$$xx' \equiv 1 [n]$$

$$xx' - 1 = kn, k \in \mathbb{Z}$$

$$\underline{\bar{x}x' - k(n) = 1}$$

$$\text{donc} \quad \Delta(x, n) = 1$$

donc les classes \bar{x} de $\mathbb{Z}/n\mathbb{Z}$ qui seront inversibles seront celles vérifiant, $x \in \{0, 1, 2, \dots, n-1\}$,

de premier avec n .

ex: si $n = 6$

$x = 0$, $\bar{0}$ non inversible.

$x = 1$ oui

$x = 3$ non

$x = 5$ oui

$x = 2$ non

$x = 4$ non

1 et 5 sont les seules classes inversibles de $\mathbb{Z}/6\mathbb{Z}$

Distinction entre les 2 cas :

n premier.

n non premier.

1°/ n premier.

Alors seule $\bar{0}$ vérifie

$$0 = kn \quad k \in \mathbb{Z}$$

$$\bar{0} = \bar{n}$$

Les autres classes vérifient $\Delta(x, n) = 1$

$$\{\mathbb{Z}/n\mathbb{Z} - \{\bar{0}\}, \times\} = \text{groupe}$$

$$(\mathbb{Z}/n\mathbb{Z}, +, \times) = \text{corps commutatif.}$$

27 n non premier

$$\exists (p, q) \in \mathbb{Z}^+ \quad / \quad n = p \cdot q \quad , \quad p \neq 1 \text{ et } q \neq 1.$$

$$p \in \{1, 2, \dots, n-1\}$$

$$q \in \{1, 2, \dots, n-1\}$$

$$\Delta(n, p) = p \neq 1$$

p non inversible.

\exists classe non inversible.

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ n'est pas un corps

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si n est premier.

25.11

Décomposition d'un entier en produit de facteurs premiers

$$N' \in \mathbb{Z} \quad , \quad N = |N'|$$

Si N est premier $= N = N$ (premier)

Si N n'est pas premier, alors $\exists p_1$ premier diviseur de N :

$$N = p_1 q_1$$

Si q_1 est premier, la décomposition est terminée.

Si q_1 n'est pas premier, $\exists p_2$ premier diviseur de q_1 ,

$$q_1 = p_2 q_2$$

$$N = p_1 p_2 q_3$$

etc ...

$$\exists q_k \text{ premier, car } N > q_1 > q_2 > \dots > q_k$$

Donc

$$N = p_1 p_2 p_3 \dots p_k \quad (k \text{ facteurs premiers})$$

$$N' = \varepsilon \cdot p_1 p_2 \dots p_k \quad \varepsilon = \pm 1$$

Cette décomposition est unique.

$$\text{Si } N = p_1 \cdot p_2 \cdot \dots \cdot p_k = p'_1 p'_2 \dots p'_m$$

Tout p_i figure dans le membre de droite.

Tout p'_j figure dans le membre de gauche.

Les décompositions coïncident

$$\text{Pratique } N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$$

Application à la recherche des diviseurs et des multiples d'un nombre

1. Les diviseurs (cf Encyclopédie 17-18 p. 15)

$$N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$$

$$N = d \cdot q \quad / \quad d \in \mathbb{N}, q \in \mathbb{N}, \text{ pour commencer}$$

$$d = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \dots \cdot p_k^{\delta_k} \quad 0 \leq \delta_i \leq \alpha_i$$

Le nombre total de diviseurs s'obtient en cherchant combien on peut faire de produits de k facteurs en extrayant chacun des facteurs d'un ensemble de cardinal $(\alpha_1 + 1)$, pour le premier, $(\alpha_2 + 1)$, pour le second, ..., $(\alpha_k + 1)$, pour le dernier.

Liste des $(\alpha_1 + 1)$ exposants possibles pour p_1 :

$$0, 1, 2, \dots, \alpha_1$$

Nombre de diviseurs de N^+

$$n = \underbrace{2(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)}_{\text{pour symétriser}}$$

Le nombre N' aura le même nombre de diviseurs (positifs ou négatifs) que N .

Bien sûr, dans \mathbb{N} , nous aurons un nombre total de diviseurs entiers naturels égal à :

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$$

2. Les multiples

$$N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$$

$$m = N \cdot q'$$

$$m = p_1^{\mu_1} \cdot p_2^{\mu_2} \cdots p_k^{\mu_k} \cdot q'' \quad \mu_i \geq \alpha_i$$

PGCD et PPCM de 2 entiers naturels décomposés en produits de facteurs premiers

$$\begin{cases} A = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \\ B = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m} \end{cases}$$

On s'est arrangé pour que les mêmes facteurs premiers interviennent dans les 2 décompositions.

$$\text{ex: } A = 2^3 \cdot 7^2 \times 3^0 \times 11^0$$

$$B = 2^4 \cdot 7 \cdot 3 \cdot 11^5$$

D = diviseur commun à A et B :

$$D = 2^{\delta_1} \cdot 7^{\delta_2} \cdot 3^{\delta_3} \cdot 11^{\delta_4}$$

$$0 \leq \delta_1 \leq 3$$

$$0 \leq \delta_2 \leq 1$$

$$0 \leq \delta_3 \leq 0$$

$$0 \leq \delta_4 \leq 0$$

$$\text{PGCD}(A, B) = 2^3 \cdot 7$$

Un multiple M commun à A et B est tel que

$$M = 2^{\mu_1} \cdot 7^{\mu_2} \cdot 3^{\mu_3} \cdot 11^{\mu_4}$$

$$\mu_1 \geq 4$$

$$\mu_3 \geq 1$$

$$\text{donc } M(A, B) = 2^4 \cdot 7^2 \cdot 3^1$$

$$\mu_2 \geq 2$$

$$\mu_4 \geq 5$$

8

Ensemble des Réels

Définition axiomatique de \mathbb{R} 1° $(\mathbb{R}, +, \times) =$ corps commutatif2° $(\mathbb{R}, \leq) =$ ensemble totalement ordonné par la relation \leq .

compatibilité

* $\forall (x, y, z) \in \mathbb{R}^3, x \leq y \vdash x + z \leq y + z$ * $\forall 0 \leq z, x \leq y \vdash xz \leq yz$ 3° Toute partie $P \subset \mathbb{R}$, $P \neq \emptyset$, P majorée, possède alors une borne supérieure dans \mathbb{R} .

Propriétés

1° Valeur absolue d'un réel x .

$$|x| = \sup(x, -x)$$

Donc $|x| = x$ si $x \geq 0$ $|x| = -x$ si $x \leq 0$

$$|xy| = |x| \cdot |y|$$

$$|x + y| \leq |x| + |y|$$

$$||x| - |y|| \leq |x + y|$$

2° (E, d) = espace métrique : c'est un ensemble muni d'une "distance".

$$\begin{aligned} d : E \times E &\longrightarrow \mathbb{R}^+ \\ (x, y) &\longmapsto d(x, y) \end{aligned}$$

- 3 propriétés
- * $d(x, y) = 0 \iff x = y$
 - * $d(x, y) = d(y, x)$
 - * $d(x, y) \leq d(x, \underline{z}) + d(\underline{z}, y)$

Ici, $E = \mathbb{R}$

$d(x, y)$? $x \in \mathbb{R}, y \in \mathbb{R}$. On convient de choisir $d(x, y) = |x - y|$, sous réserve de vérification :

$$d(x, y) = |x - y|$$

- * $|x - y| = 0 \iff x = y$
- * $|x - y| = |y - x|$
- * $|x - y| \leq |x - z| + |z - y|$?

En effet

$$x - y = (x - z) + (z - y)$$

$$|(x - z) + (z - y)| \leq |x - z| + |z - y|$$

Construction du corps \mathbb{Q} = c'est un sous-corps de \mathbb{R}

$$\mathbb{Q} / \mathbb{Z} \times \mathbb{Z}^*$$

$$a \in \mathbb{Z} ; b \in \mathbb{Z}^*$$

$$\underbrace{(a, b)}_{\text{fraction}} \in \mathbb{Z} \times \mathbb{Z}^*$$

$$x = (a, b) \in \mathbb{R} / x \times b = a$$

On crée ainsi de nouveaux nombres, non entiers relatifs qui jouiraient de la propriété ci-dessus.

Mais il existe plusieurs couples tels que (a, b) qui répondraient à la même définition ; c'est-à-dire :

$$x \times b = a$$

$$x' \times b = a$$

$$x'' \times b = a$$

On remarque, dans le cas où x, x', x'' sont entiers relatifs, que les couples qui les représentent vérifient $a b' = b a'$ avec 1^{er} couple = (a, b)

$$2^{\text{e}} \text{ couple} = (a', b')$$

Alors on définit dans $\mathbb{Z} \times \mathbb{Z}^*$ une relation binaire :

$$(a, b) \mathcal{R} (a', b') \iff a b' = b a'$$

ex: $(a, b) = (4, 3)$

$(a', b') = (-20, -15)$

$4 \times (-15) = 3(-20)$

On montre que \mathcal{R} est une relation d'équivalence.

Donc il existe des classes d'équivalence. Chacune est appelée nombre rationnel

ex: $(4, 3) \mathcal{R} (-20, -15)$

\exists nombre rationnel qu'on convient de nommer en utilisant les plus petites valeurs absolues de a et b

ex: ici $(4, 3)$, mieux $\frac{4}{3}$

$\Delta(4, 3) = 1$ tandis que $\Delta(-20, -15) = 5$

On dit que la fraction $\frac{4}{3}$ est irréductible

Borne supérieure et borne inférieure

Définition d'une borne supérieure B.S.:

1° BS est un majorant

$\forall a, a \in P, a \leq BS$

2° BS est le plus petit des majorants

$\exists m, m \in (\text{Ens. des majorants}) / m < BS$

Une borne inférieure BI vérifie.

$$1^\circ \forall a \in P, BI \leq a$$

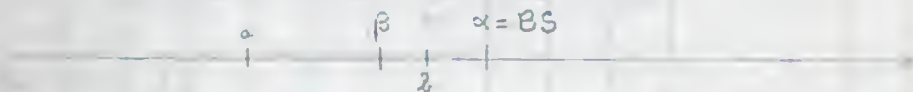
$$2^\circ \exists m \in (\text{Ens. des mineurs}) / BI < m$$

P est dite bornée si P admet une BS et une BI.

Bien entendu, dans ce cas $BI \leq BS$ (voir $BI \leq a \leq BS$)

3.12

Caractérisation d'une borne supérieure.



$$\alpha = BS \text{ de } P, P \subset \mathbb{R}$$

$$\forall a \in P, a \leq \alpha$$

$$\forall \beta, \beta \in \mathbb{R}, \beta < \alpha, \exists \gamma, \gamma \in P / \beta < \gamma \leq \alpha$$

En d'autres termes

$$\beta = \alpha - \varepsilon, \varepsilon \in \mathbb{R}_+^*$$

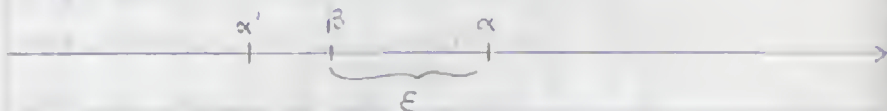
$$\forall \varepsilon \in \mathbb{R}_+^*, \exists \gamma, \gamma \in P / \alpha - \varepsilon < \gamma \leq \alpha$$

Inversement : si un majorant de P possède la propriété ci-dessus, est-ce, à coup sûr, le plus petit majorant donc est-ce BS?

$$\text{Donc : } \forall a \in P, a \leq \alpha$$

$$\forall \varepsilon \in \mathbb{R}_+^*, \exists \gamma \in P / \alpha - \varepsilon < \gamma \leq \alpha$$

S'il existait un autre majorant de P , et $\alpha' < \alpha$
alors



Il suffit de choisir un ϵ tel que $\epsilon < \alpha - \alpha'$
alors $\exists b / \alpha - \epsilon < b \leq \alpha \quad b \in P$

$$\underline{\alpha'} < \alpha - \epsilon < \underline{b} \leq \alpha$$

on aurait $\alpha' < b$
et, α' majorant } incompatibilité.

Donc $\nexists \alpha'$, $\alpha' < \alpha$ et α' majorant de P .

Donc $\alpha = BS$.

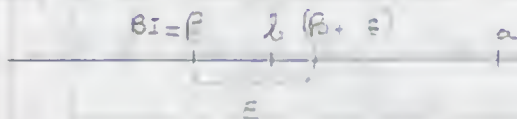
La propriété ci-dessus constitue donc un critère de
borne supérieure de P .

De même, critère de borne inférieure pour P .

$$1^\circ \forall a, a \in P, \beta \leq a, \quad \beta = BI$$

$$2^\circ \forall \epsilon \in \mathbb{R}_+^*, \exists b, b \in P /$$

$$\beta \leq b < \beta + \epsilon$$



Remarque:

BS , (ou BI) fait ou non partie de P , on ne le sait

pas à l'avance. Si oui, BS (resp. BI) est le plus grand élément de P (resp. le plus petit élément de P)

Intervalle de \mathbb{R}

1° Définition :

$$[a, b] : (a, b) \in \mathbb{R}^2$$

$$[a, b] = \{x, x \in \mathbb{R} / a \leq x \leq b\}$$

$$[a, b[= \{x, x \in \mathbb{R} / a \leq x < b\}$$

$$[a, a] = \{a\}$$

$$[a, a[= \emptyset =]a, a] =]a, a[$$

$$[a, +\infty[= \{x, x \in \mathbb{R} / a \leq x\}$$

$$]-\infty, b] = \{x, x \in \mathbb{R} / x \leq b\}$$

$$]-\infty, +\infty[= \mathbb{R}$$

On adjoint à \mathbb{R} l'ensemble $\{-\infty; +\infty\}$ qui n'est pas une ^{paire} ~~couple~~ de nombres, mais qui permet de former :

$$\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty; +\infty\} \quad \text{avec} \quad \mathbb{R} \cap \{-\infty, +\infty\} = \emptyset$$

De plus, on ordonne $\overline{\mathbb{R}}$ ainsi :

$$1^\circ \forall (x, y) \in \mathbb{R}^2, \quad x \leq y \quad \text{est la relation connue.}$$

$$2^\circ \forall x \in \overline{\mathbb{R}}, \quad x \leq +\infty$$

$$3^\circ \forall x \in \overline{\mathbb{R}}, \quad -\infty \leq x$$

2° Propriété d'un intervalle I de \mathbb{R} , $I \neq \emptyset$.

$\forall (x, y) \in I^2$, $[x, y] \subset I$ $x \leq y$
(= sans intérêt)

ex: $I =]a, +\infty[$

$a < x < y < +\infty$

$\forall z \in [x, y]$, alors $z \in I$

3° Inversement

Soit une partie P de \mathbb{R} , non vide, telle que, $\forall (x, y) \in P^2$,
 $x \leq y$, alors $[x, y] \subset P$, alors on va montrer que
 P est un intervalle.

1 \rightarrow * supposons que P est bornée:

$\exists! \alpha = \text{BS}$, $\exists! \beta = \text{BI}$ de P .

On voit vite que $P \subset \underline{[\beta, \alpha]}$

Inversement, $\forall z \in \mathbb{R}$, $z \in]\beta, \alpha[$



$\forall z \in]\beta, \alpha[$, $\varepsilon = \alpha - z$, alors $\exists y \in P$, $z < y \leq \alpha$

$\varepsilon' = z - \beta$, alors $\exists x \in P$, $\beta \leq x < z$

Donc $\beta \leq x < z < y \leq \alpha$

D'après l'hypothèse : $[x, y] \subset P \vdash \underline{z \in P}$

Donc $P = [\beta, \alpha]$ ou $] \beta, \alpha]$ ou $] \beta, \alpha[$ ou $[\beta, \alpha[$,
 P est un intervalle.

Remarque: Si $\beta = \alpha$, alors $P \neq \emptyset$ coïncide avec $\{\alpha\}$,
 donc $P = [\alpha, \alpha]$ et $P = \text{intervalle}$.

Dans le cas général : $\alpha \neq \beta$, l'hypothèse : P non vide,
 intervient quand on annonce : $\exists y \in P, z < y \leq \alpha$

2 \rightarrow * Supposons que P est bornée supérieurement et non bornée inférieurement.

$\forall u \in P, u \leq \alpha$, donc $P \subset]-\infty, \alpha]$.

$\forall z \in]-\infty, \alpha[$



$\varepsilon = \alpha - z$, $\exists y \in P / z < y \leq \alpha$

$\exists x \in P / x < z$ (voir P non bornée inférieurement)

$-\infty < \underline{x} < z < y \leq \alpha$

$z \in]x, y[\vdash z \in P$

$\forall z \in]-\infty, \alpha[, z \in P$

Donc $P =]-\infty, \alpha[$ ou $]-\infty, \alpha]$.

3 \rightarrow * Si P admet $\beta = BI$ et non $\alpha = BS$, alors

$$P \subset [\beta, +\infty[$$

$$\forall z \in]\beta, +\infty[$$



$$\exists x \in P / \beta \leq x < z$$

$$\exists y \in P / z < y \quad (\text{voir } \nexists \alpha = BS)$$

$$\beta \leq x < z < y < +\infty$$

donc $z \in P$

$$P = [\beta, +\infty[\text{ ou }]\beta, +\infty[$$

4 \rightarrow * $\nexists \alpha = BS$, $\nexists \beta = BI$ pour la partie P .

$$P \subset \mathbb{R}$$

$$\forall z \in \mathbb{R} =]-\infty, +\infty[$$

$$\exists x < z, \exists y > z$$

$$-\infty < x < z < y < +\infty$$

donc $z \in P$

donc $\underline{P = \mathbb{R}}$

11.12

\mathbb{R} est archimédien (propriété d'Archimède) $\forall x \in \mathbb{R} \exists n \in \mathbb{N} / x < n$

$$\sum \forall x \in \mathbb{R}_+^*, \forall y \in \mathbb{R}, \exists n \in \mathbb{N} / y < nx$$

Conséquence.

$$P = \{ p, p \in \mathbb{N} / p > x, x \in \mathbb{R} \text{ et } x \text{ donné} \}$$

* $P \neq \emptyset$ (\mathbb{R} est archimédien)

* P est minorée par x .

* \exists BI pour P , mais il existe plus petit élément

Donc BI = ce plus petit élément ; soit n' .

$$\begin{cases} n' > x \\ \nexists p, p \in P ; p < n' \end{cases}$$

$$\exists (n'-1) \in \mathbb{N}, n'-1 \notin P$$

$$\underbrace{(n'-1)}_n \leq x$$

$\exists n \leq x$ tel que

$$n \leq x < n+1$$

$$\text{ex: } x = 5,6 \text{ alors } n = 5$$

$$x = 5, \text{ alors } n = 5$$

Remarque: Il se peut qu'on introduise un jour, dans

à l'aide d'un algorithme on trouve un nombre rationnel qui s'écrit
 $3,1415926535$

un problème, un entier m tel que : $\underbrace{m}_{l-1} < x \leq \underbrace{m+1}_l$

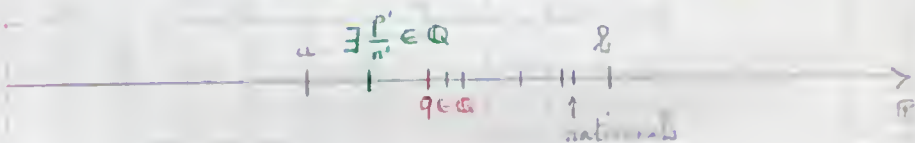
Par ex: $x = 5,6 \quad 5 < 5,6 < 6$

$x = 5 \quad 4 < 5 \leq 5$

\mathbb{Q} (ens des rationnels) est dense dans \mathbb{R}

1° $\forall (a,b) \in \mathbb{R}^2, a < b, \exists \frac{p}{n} \in \mathbb{Q}$
 tel que $a < \frac{p}{n} < b$

2° \exists infinité de rationnels analogues à $\frac{p}{n}$.



valeur approchée à 10^{-n} près d'un réel.

$\underbrace{6,45}_{\text{v.a. par défaut de } 6,453} < 6,453 < \underbrace{6,46}_{\text{v.a. par excès de } 6,453}$

$\underbrace{3,1415926}_{\alpha} < \pi < \underbrace{3,1415927}_{\beta}$
 $\beta - \alpha = 10^{-7}$

notion de limite 1° d'un nombre x d'un réel a

2°

3° d'un réel a

Revenons à $x = 6,453$

$$x \cdot 10^3 = 6453$$

$$x \cdot 10^2 = 645,3$$

$$645 \leq 645,3 < 646$$

$$p_n \leq x \cdot 10^2 < p_n + 1$$

$$\underbrace{p_n \cdot 10^{-2}} \leq x < (p_n + 1) 10^{-2}$$

valeur approchée par défaut de x à 10^{-2} près.

Valeurs approchées par défaut et par excès à 10^{-k} près
($k \in \mathbb{N}$) (cf C1 172).

$\forall x \in \mathbb{R}$, $\forall k \geq 0$, $\exists p_k$ unique tel que

$$p_k \leq 10^k x < p_k + 1$$

p_k est la partie entière de $10^k x$.

On a :

$$p_k \cdot 10^{-k} \leq x < (p_k + 1) 10^{-k}$$

$a_k = p_k \cdot 10^{-k}$ est appelé valeur approchée par défaut à 10^{-k} près de x .

$b_k = (p_k + 1) 10^{-k}$ est appelé valeur approchée par excès à 10^{-k} près de x .

Rappel

$$A = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \quad (a, b, c, d) \in \mathbb{R}^4$$

$$\mathcal{M}_2 = \left\{ \text{ensemble des } A, \forall (a, b, c, d) \in \mathbb{R}^4 \right\}$$

$(\mathcal{M}_2, +, \cdot)$ = anneau unitaire non commutatif.

On rappelle l'isomorphisme d'anneaux entre $(\mathcal{L}(E), +, \cdot)$ et $(\mathcal{M}_2, +, \cdot)$, $\mathcal{L}(E)$ = ensemble des endomorphismes de E (dimension 2).

Étude de l'ensemble \mathbb{C} des matrices de la forme $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$

$$z = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

1° $(\mathbb{C}, +)$ = groupe commutatif

$$\forall z_1 \in \mathbb{C}, \forall z_2 \in \mathbb{C}, z_1 + (-z_2) \in \mathbb{C}$$

En effet :

$$z_1 + (-z_2) = \begin{bmatrix} a_1 - a_2 & -b_1 + b_2 \\ b_1 - b_2 & a_1 - a_2 \end{bmatrix} = \begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix} \in \mathbb{C}$$

$$\mathbb{C} \neq \emptyset, \text{ exemple } I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$27 \left(\mathbb{C}^* = \mathbb{C} - \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \times \right) = \text{groupe commutatif}$$

$$z_1 \times z_2 = \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix} = \underbrace{\begin{bmatrix} a_1 a_2 - b_1 b_2 & -a_1 b_2 - a_2 b_1 \\ a_2 b_1 + a_1 b_2 & -b_1 b_2 + a_1 a_2 \end{bmatrix}}_{\in \mathbb{C}}$$

Il est suffisant maintenant de montrer l'existence de $z^{-1} \in \mathbb{C}^*, \forall z \in \mathbb{C}^*$

$$z \times z^{-1} = z^{-1} \times z = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

On trouve $z^{-1} : z^{-1} = \frac{1}{a^2 + b^2} \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$

$$z^{-1} = \begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix} \in \mathbb{C}$$

2 12

De plus \times est commutative dans \mathbb{C} .

$$z_1 \times z_2 = z_2 \times z_1 = \begin{bmatrix} a_1 a_2 - b_1 b_2 & -a_1 b_2 - a_2 b_1 \\ a_2 b_1 + a_1 b_2 & a_1 a_2 - b_1 b_2 \end{bmatrix}$$

L'échange des indices 1 et 2 conserve la matrice-produit.

(\mathbb{C}^*, \times) = groupe commutatif

Z

En résumé : $(\mathbb{C}, +, \times) = \text{corps commutatif}$

De plus il est un sous-anneau commutatif, unitaire de l'anneau M_2 . De plus \mathbb{C} étant un corps est un anneau intègre:

$$z_1 \times z_2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \longmapsto z_1 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \text{ ou } z_2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

On appelle \mathbb{C} le corps des nombres complexes.

\mathbb{R} est un sous-corps de \mathbb{C}

Soit $S \subset \mathbb{C} / S$ est l'ensemble des matrices du type $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$, dites 1° matrices diagonales.
2° matrices scalaires

Soit φ une application de \mathbb{R} vers S

$$\varphi: \mathbb{R} \longrightarrow S$$

$$a \longmapsto \varphi(a) = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$$

$$a' \longmapsto \varphi(a') = \begin{bmatrix} a' & 0 \\ 0 & a' \end{bmatrix}$$

$$a + a' \longmapsto \varphi(a + a') = \begin{bmatrix} a + a' & 0 \\ 0 & a + a' \end{bmatrix}$$

$$\text{donc } \underline{\varphi(a + a') = \varphi(a) + \varphi(a')}$$

φ étant visiblement bijective, φ est un isomorphisme entre $(\mathbb{R}, +)$ et $(S, +)$. De plus, c'est un

isomorphisme de groupe

$$\text{Dc plus } a \mapsto \varphi(a) = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$$

$$a' \mapsto \varphi(a') = \begin{bmatrix} a' & 0 \\ 0 & a' \end{bmatrix}$$

$$a \times a' \mapsto \varphi(a \times a') = \begin{bmatrix} aa' & 0 \\ 0 & aa' \end{bmatrix}$$

$$\varphi(a) \stackrel{\downarrow}{\times} \varphi(a') = \begin{bmatrix} aa' & 0 \\ 0 & aa' \end{bmatrix}$$

$$\text{donc } \underline{\varphi(a \times a') = \varphi(a) \times \varphi(a')}$$

φ est encore un isomorphisme entre les 2 groupes multiplicatifs \mathbb{R}^* et S^*

φ est un isomorphisme de corps

$$\varphi: \mathbb{R} \longrightarrow S$$

On convient de dire que $S = \mathbb{R}$ (on identifie \mathbb{R} à S)

$$\mapsto \varphi = \text{Id}$$

$S = \text{corps}$; $S \subset \mathbb{C} (\text{corps})$

\mathbb{R} est un sous-corps de \mathbb{C}

\mathbb{C} est un espace vectoriel sur \mathbb{R}

$$\forall \lambda \in \mathbb{R}, \forall z \in \mathbb{C}$$

$$\lambda \cdot z = z'$$

$$\text{En effet } \lambda \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} \lambda a & -\lambda b \\ \lambda b & \lambda a \end{bmatrix} = z'$$

On peut aussi poser $\lambda = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}$, $z = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$, on fait le produit de 2 matrices, on trouve z' .

$(\mathbb{C}, +)$ = groupe commutatif

$$\text{De plus } \forall \lambda \in \mathbb{R}, \forall (z, z') \in \mathbb{C}^2, \lambda(z + z') = \lambda z' + \lambda z$$

$$\forall (\lambda, \mu) \in \mathbb{R}^2, \forall z \in \mathbb{C}^2, (\lambda + \mu)z = \lambda z + \mu z$$

$$\forall (\lambda, \mu) \in \mathbb{R}^2, \forall z \in \mathbb{C}, \lambda \mu z = \lambda(\mu z)$$

$$\forall z \in \mathbb{C}, 1 \cdot z = z$$

Recherche d'une base

$$z = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = a \underbrace{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}_{\text{c'est le réel } 1} + b \underbrace{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}}_i$$

i est un nombre complexe

La partie $\{1, i\}$ est donc génératrice de \mathbb{C} puisque

$$\forall z \in \mathbb{C}, z = a \cdot 1 + b \cdot i \quad (a, b) \in \mathbb{R}^2$$

Est-elle libre ?

Oui, si et seulement si

$$\alpha \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \beta \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \vdash \alpha = \beta = 0$$

$$\text{Gr} \quad \begin{cases} \alpha \cdot 1 + \beta \cdot 0 = 0 \vdash \alpha = 0 \\ \alpha \cdot 0 + \beta \cdot 1 = 0 \vdash \beta = 0 \\ \alpha \cdot 0 + \beta \cdot (-1) = 0 \vdash \beta = 0 \\ \alpha \cdot 1 + \beta \cdot 0 = 0 \vdash \alpha = 0 \end{cases} \quad \alpha = \beta = 0, \text{ oui}$$

$(1, i) = \text{base de } \mathbb{C}$

Conséquence :

$$\forall z \in \mathbb{C}, \exists ! (a, b) \in \mathbb{R}^2 / z = a + bi$$

Conséquence 2 : $z = z' \vdash a = a' \text{ et } b = b'$

puisque $z = a + bi$

$$z' = a' + b'i \quad \text{et } \exists ! (a, b) \in \mathbb{R}^2$$

$$\alpha + \beta \cdot 1 = 0 \vdash \alpha = \beta = 0$$

Carri de \mathbb{C}

$$i^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \underbrace{\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}}_{\in S = \mathbb{R}}$$



$$i^2 = -1$$

$$x = -1 \quad \text{ou} \quad x = -2 \quad \text{ou} \quad x = 2$$

13 12

Application : $x^2 + x + 1 = 0$ à résoudre dans \mathbb{C}

$$x^2 + x + 1 = 0$$

$$\left(x + \frac{1}{2}\right)^2 - \frac{1}{4} + 1 = 0$$

$$\left(x + \frac{1}{2}\right)^2 = -\frac{3}{4} = \frac{3}{4}(-1) = \frac{3}{4}i^2$$

$$\left(x + \frac{1}{2}\right)^2 = \frac{3}{4}i^2 = 0$$

$$\text{d'où} \quad \left(x + \frac{1}{2} + \frac{\sqrt{3}}{2}i\right)\left(x + \frac{1}{2} - i\frac{\sqrt{3}}{2}\right) = 0$$

$$\begin{cases} x' = -\frac{1}{2} - i\frac{\sqrt{3}}{2} \\ x'' = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \end{cases}$$

$$x = \frac{-1 \pm i\sqrt{3}}{2}$$

2^e exemple

$$x^2 - x + 2 = 0$$

$$\left(x - \frac{1}{2}\right)^2 - \frac{1}{4} + \frac{8}{4} = 0$$

$$\left(x - \frac{1}{2}\right)^2 = -\frac{7}{4} = \frac{7}{4} i^2$$

$$\left(x - \frac{1}{2} + \frac{\sqrt{7}}{2} i\right) \left(x - \frac{1}{2} - \frac{\sqrt{7}}{2} i\right) = 0$$

$$x = \frac{1 \pm i\sqrt{7}}{2}$$

les 4 opérations

$$1^o \quad z = a + bi \quad ; \quad z' = a' + b'i$$

$$z + z' = (a + a') + (b + b')i$$

$$2^o \quad z - z' = (a - a') + (b - b')i$$

$$3^o \quad z \times z' = zz'$$

$$zz' = (a + bi)(a' + b'i)$$

$$= (aa' - bb') + (ab' + ba')i$$

4°/

$$\frac{1}{z'} = \frac{-1}{a' + b'i} = \frac{a' - b'i}{a'^2 + \underset{\uparrow}{b'^2}} \quad , \text{ si } z' \neq 0 \Rightarrow a' \neq 0 \text{ ou } b' \neq 0$$

$$\frac{1}{z'} = \frac{a'}{a'^2 + b'^2} - \frac{b'}{a'^2 + b'^2} i$$

On retrouve évidemment la matrice inverse de celle attachée à z'

$$z' = \begin{bmatrix} a' & -b' \\ +b' & a' \end{bmatrix} \quad \frac{1}{z'} = \frac{1}{a'^2 + b'^2} \begin{bmatrix} a' & b' \\ -b' & a' \end{bmatrix}$$

En on déduit $\frac{z}{z'} = \frac{1}{z'}$, $z' \neq 0$

$$\frac{z}{z'} = z \cdot \frac{1}{z'}$$

Nombre complexe conjugué d'un nombre complexe donné

C'est $\bar{z} = a - bi$ dès que $z = a + bi$

$$* f: \mathbb{C} \rightarrow \mathbb{C}$$

$$z \mapsto \bar{z}$$

$$a + bi \mapsto f(z) = a - bi$$

* f est bijective.

* De plus, $\forall z \in \mathbb{C}, f \circ f(z) = z$

$$\boxed{\bar{\bar{z}} = z} \quad (1)$$

$\bar{}$ est donc involutive.

$$\begin{aligned} * \quad \bar{z} &\longmapsto \overline{\bar{z}} \\ \bar{z}' &\longmapsto \overline{\bar{z}'} \\ \overline{z+z'} &\longmapsto \overline{\overline{z+z'}} \end{aligned}$$

$$\begin{aligned} \overline{z+z'} &= \overline{(a+a') + (b+b')i} \\ &= a+a' - (b+b')i \\ &= (a-bi) + (a'-b'i) \end{aligned}$$

$$\overline{z+z'} = \bar{z} + \bar{z}'$$

$$\boxed{\overline{z+z'} = \bar{z} + \bar{z}'} \quad (2)$$

$$\begin{aligned} * \quad \overline{z z'} &= \overline{(aa' - bb') + (a'b + ab')i} \\ &= (aa' - bb') - (a'b + ab')i \\ \bar{z} \cdot \bar{z}' &= (a-bi)(a'-b'i) \\ &= (aa' - bb') + (ab' + ba')i \end{aligned}$$

$$\boxed{\overline{z z'} = \bar{z} \bar{z}'} \quad (3)$$

$\bar{}$ est donc un automorphisme involutif du corps \mathbb{C} .

Représentation géométrique d'un nombre complexe

On associe à \mathbb{C} , soit \vec{P} vectoriel euclidien, soit P affixe euclidien :

$$\begin{array}{lcl}
 b_1: \mathbb{C} \rightarrow \vec{P} & & b_2: \mathbb{C} \rightarrow P = (O, \vec{P}) \\
 z \mapsto \vec{w} & & z \mapsto \underbrace{M}_{\text{tel que:}} \\
 z = \underline{a} + \underline{b}i & \vec{w} = \underline{a}\vec{u} + \underline{b}\vec{v} & \vec{OM} = \vec{w} = \underline{a}\vec{u} + \underline{b}\vec{v} \\
 (\vec{u}, \vec{v}) = \text{base orthonormée de } \vec{P} & &
 \end{array}$$

Remarques

A = image de z .

B = image de z' .

z = affixe de A .

z' = affixe de B .

\vec{OA} = image de z , aussi.

z = affixe de \vec{OA} .

$$z + z' = (a + a') + (b + b')i$$

$$= \text{affixe de } S \in P$$

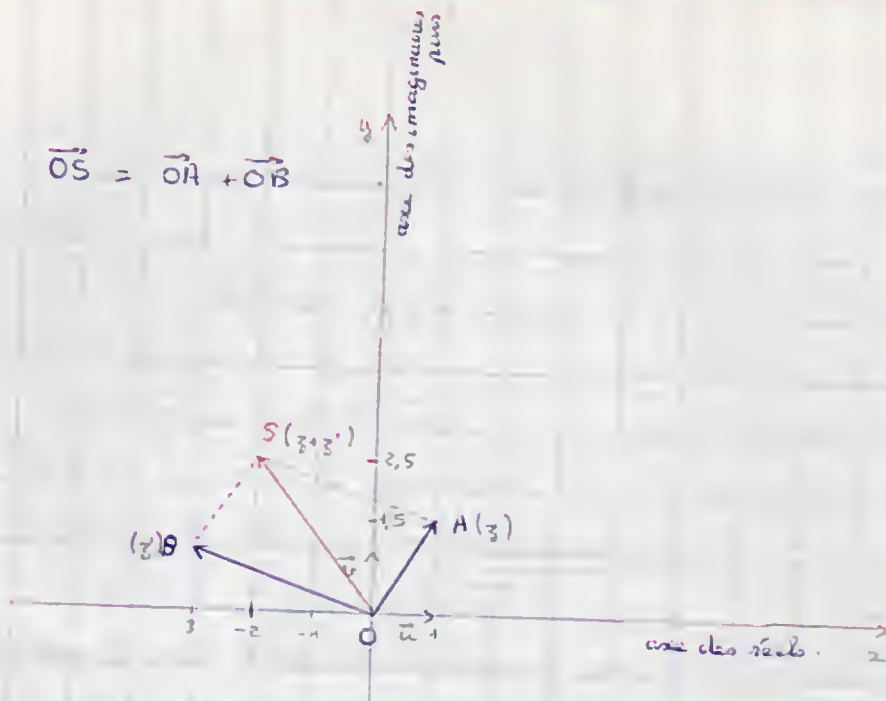
$$= \text{" de } \vec{OS} \in \vec{P}$$

$$\vec{OS} = (a + a')\vec{u} + (b + b')\vec{v}$$

$$= \underbrace{(a\vec{u} + b\vec{v})}_{\vec{OA}} + \underbrace{(a'\vec{u} + b'\vec{v})}_{\vec{OB}}$$

l'affixe de S est la somme
de l'affixe de A et de l'affixe de B .

$$\vec{OS} = \vec{OA} + \vec{OB}$$



\vec{BS} a, comme \vec{OA} , et comme A , pour affixe z

De plus $\vec{OA} = \vec{OS} - \vec{OB}$

$$(a, b) = (a + a', b + b') - (a', b')$$

ou encore : $\vec{BS} = \vec{OS} - \vec{OB}$

donc :

$$\text{affixe } \vec{BS} = \text{affixe } S - \text{affixe } B$$

12

Module d'un nombre complexe

$$z = a + bi$$

$$\bar{z} = a - bi$$

$$z \bar{z} = a^2 + b^2 = r^2$$

$$|z| = \sqrt{z \bar{z}} = \sqrt{a^2 + b^2}$$

$$r = |z|$$

Remarque

$$|z| = \|\vec{OM}\| \text{ où } M(z)$$

Toutes les propriétés de $\|\vec{v}\|$, $\vec{v} \in \vec{E}$ espace vect. euclidien se retrouvent donc à propos de $|z|$, $z \in \mathbb{C}$ et en particulier : $|z_1 + z_2| \leq |z_1| + |z_2|$

(voir dans \vec{E} inégalité triangulaire de Minkowski)

Par contre, avec $\bar{\cdot}$ opération \times , dans \mathbb{C}

$$\begin{aligned} |z_1 \cdot z_2| &= \sqrt{z_1 z_2 \cdot \overline{z_1 z_2}} \\ &= \sqrt{z_1 z_2 \cdot \bar{z}_1 \bar{z}_2} \\ &= \sqrt{z_1 \bar{z}_1 \cdot z_2 \bar{z}_2} \\ &= \sqrt{z_1 \bar{z}_1} \cdot \sqrt{z_2 \bar{z}_2} \\ &= |z_1| \cdot |z_2| \end{aligned}$$

$$\lambda: \mathbb{C} \longrightarrow \mathbb{R}^+$$

$$z_1 \longmapsto |z_1|$$

$$z_2 \longmapsto |z_2|$$

$$z_1 \times z_2 \longmapsto |z_1 z_2| = |z_1| \times |z_2|$$

λ est un homomorphisme (donc non bijectif) de (\mathbb{C}, \times) vers (\mathbb{R}^+, \times)

Si l'on cherche le noyau de λ , c'est-à-dire l'ensemble des complexes dont l'image par λ est l'élément neutre de \times dans \mathbb{R}^+ , on trouve tous les complexes de module 1, donc de matrices du type $\begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix}$ et $\alpha^2 + \beta^2 = 1$, $z = \alpha + \beta i$

Nous reconnaissons les matrices des rotations vectorielles de \vec{P} (plan d'Argand-Cauchy)

Notons U ce noyau :

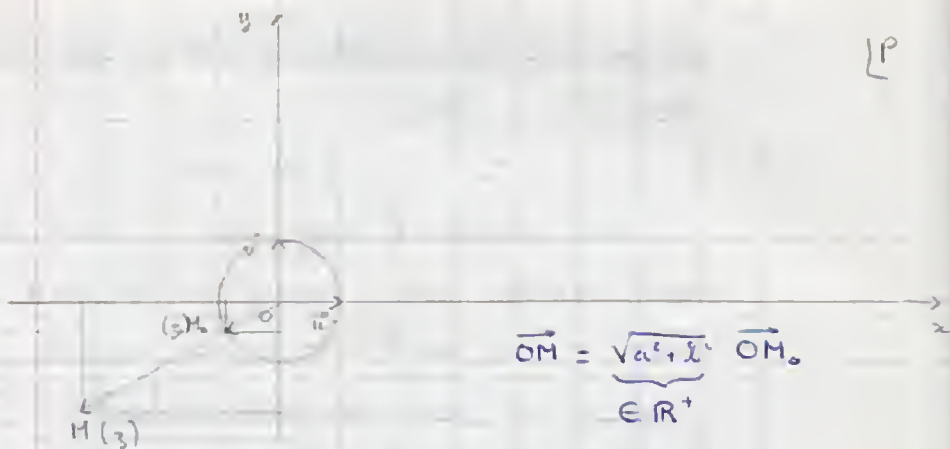
$$U = \left\{ z, z \in \mathbb{C}, / |z| = \sqrt{\alpha^2 + \beta^2} = 1 \right\}$$

Application

$$\forall z \in \mathbb{C}, \exists z_0 \in U / \underline{z = |z| \cdot z_0}$$

$$z = a + bi$$

$$z_0 = \frac{a}{|z|} + \frac{b}{|z|} i \quad \text{ou} \quad z_0 = \frac{1}{\sqrt{a^2 + b^2}} (a + bi)$$



Remarque

\vec{OM}_0 n'est autre que l'unique vecteur unitaire de la droite affine (OM) , qui est orienté comme \vec{OM} .

Distance définie sur \mathbb{C}
voir ligne.

Racines carrées d'un nombre complexe

Soit Z donné, $Z \in \mathbb{C}$

$$\underline{Z = a + bi}, \quad (a, b) \in \mathbb{R}^2$$

Existe-t-il $z \in \mathbb{C} / \underline{z^2 = Z}$?

Posez $z = x + yi$, $(x, y) \in \mathbb{R}^2$.

Le problème revient à chercher s'il existe x et y réels

$$(x + yi)^2 = a + bi$$

$$(x^2 - y^2) + (2xy)i = a + bi$$

$$\begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases}$$

$$\begin{cases} x^2 - y^2 = a \\ 4x^2y^2 = b^2 \\ \text{Sgn } xy = \text{Sgn } b \end{cases}$$

$$\begin{cases} x^2 + (-y^2) = a \\ x^2 \times (-y^2) = -\frac{b^2}{4} \\ \text{Sgn } xy = \text{Sgn } b \end{cases}$$

Posons $x^2 = X$

$$-y^2 = Y$$

X et Y , s'ils existent, sont les racines de l'équation :

$$X^2 - aX - \frac{b^2}{4} = 0 \quad (1)$$

0.12

$\Delta = a^2 + b^2 \geq 0$; d'ailleurs les termes extrêmes sont de signe contraire $\vdash \exists (X', X'') / \underbrace{X' \leq 0}_{-y^2} \leq \underbrace{0 \leq X''}_{x^2}$

$$\forall (a, b) \in \mathbb{R}^2 \vdash \forall Z \in \mathbb{C},$$

$$\exists! (X'', -X') = (x^2, y^2)$$

$$x^2 = X'' \vdash x = \pm \sqrt{X''}$$

$$y^2 = -X' \vdash y = \pm \sqrt{-X'}$$

et on se souvient que

$$\text{Sgn } xy = \text{Sgn } b$$

Or le signe de b est connu (sauf si $b=0$) donc 2 associations et 2 couplement de signes

$$b > 0 \quad \vdash \quad \begin{cases} x = \sqrt{x''} \text{ et } y = \sqrt{-x'} \\ \text{ou} \\ x = -\sqrt{x''} \text{ et } y = -\sqrt{-x'} \end{cases}$$

$$b < 0 \quad \vdash \quad \begin{cases} x = -\sqrt{x''} \text{ et } y = \sqrt{-x'} \\ \text{ou} \\ x = \sqrt{x''} \text{ et } y = -\sqrt{-x'} \end{cases}$$

$$z = x + yi \quad \exists z' \text{ et } z'', \text{ racines carrées de } Z = a + bi$$

$$z'' = -z'$$

Si $b=0$, $x^2 - ax = 0$ voir (1)

$$x(x-a) = 0$$

$$\begin{cases} x' = 0 \\ x'' = a \end{cases}$$

* $a > 0$ $\vdash x^2 = a$ et $-y^2 = 0$

donc $x = \pm \sqrt{a}$; $y = 0$

$$\begin{cases} z' = \sqrt{a} + 0i = \sqrt{a} \in \mathbb{R} \\ z'' = -\sqrt{a} + 0i = -\sqrt{a} \in \mathbb{R} \end{cases}$$

d'ailleurs : $Z = a + 0i = a > 0$

On savait que $z = \pm \sqrt{a}$

* $a < 0$ $\vdash -y^2 = a$ et $x^2 = 0$

donc $x=0$, $y = \pm \sqrt{-a}$

$$\begin{cases} z' = +i\sqrt{-a} \\ z'' = -i\sqrt{-a} \end{cases}$$

d'ailleurs $Z = a + \underbrace{b}_0 i = a < 0$

$$\begin{aligned} \text{car } Z &= -(-a) = (-1)(-a) \\ &= (-a)(-1) \\ &= \underbrace{(-a)}_{>0} i^2 \end{aligned}$$

$$\begin{cases} z' = -i\sqrt{-a} \\ z'' = i\sqrt{-a} = -z' \end{cases}$$

* $a=0$ (et $b=0$)

$$x^2 = 0$$

$$x' = x'' = 0$$

$$x^2 = -y^2 = 0 \quad \vdash \quad x=y=0 \quad \vdash \quad x+yi = 0 = z' = z''$$

(et aussi $z'' = -z'$)

Équations du second degré.

$$ax^2 + bx + c = 0 \quad \text{dans } \mathbb{C}$$

$$(a \neq 0)$$

1° Supposons $(a, b, c) \in \mathbb{R}^3$; $x \in \mathbb{C}$.

* $\Delta = b^2 - 4ac \in \mathbb{R}$

$\Delta > 0$

alors $x = \frac{-b \pm \sqrt{\Delta}}{2a} \in \mathbb{R}$

* $\Delta = 0$

alors $x = -\frac{b}{2a} \in \mathbb{R}$.

* $\Delta < 0$

alors $\Delta = -\underbrace{(4ac - b^2)}_{-\Delta > 0}$

$4ac - b^2 \in \mathbb{R}^+$ et. On peut écrire $\Delta = (-\Delta)^{\frac{1}{2}}$

$\Delta = z_1^2 = z_2^2$ et $z_2 = -z_1$

$z_1 = i\sqrt{-\Delta}$ $z_2 = -i\sqrt{-\Delta}$

Les formules apprises dans \mathbb{R} ($x \in \mathbb{R}$) sont encore valables dans \mathbb{C} , à condition de remplacer $\pm\sqrt{\Delta}$

par $+z_1$ ou $+z_2$

$x' = \frac{-b + z_1}{2a}$

$x'' = \frac{-b + z_2}{2a}$

} avec $z_2 = -z_1$

$\Delta < 0$

$x' = \frac{-b + i\sqrt{-\Delta}}{2a}$

$x'' = \frac{-b - i\sqrt{-\Delta}}{2a}$

$$2^\circ \quad (a, b, c) \in \mathbb{C}^3$$

On peut, comme ci-dessus, calculer $\Delta = b^2 - 4ac \in \mathbb{C}$
 Il existe z_1 et $z_2 \in \mathbb{C}$ telles que $z_2 = -z_1$

$$z_1^2 = z_2^2 = b^2 - 4ac$$

Mais, dans le corps \mathbb{C} , on peut utiliser les résultats classiques dans \mathbb{R}

$$\begin{cases} x' = \frac{-b + z_1}{2a} \\ x'' = \frac{-b + z_2}{2a} \end{cases} \quad \text{et } z_2 = -z_1$$

$$\forall (a, b, c) \in \mathbb{C}^* \times \mathbb{C} \times \mathbb{C}$$

$$* \quad b^2 - 4ac \neq 0 \quad \exists x', x'' / x'' \neq x'$$

$$* \quad b^2 - 4ac = 0 \quad \exists! x' = x'' = \frac{-b}{2a} \in \mathbb{C}$$

On peut aussi reprendre la décomposition en carrés classique.

$$a \left(x^2 + \frac{b}{a}x + \frac{c}{a} \right) = 0$$

$$\left(x + \frac{b}{2a} \right)^2 - \frac{b^2}{4a^2} + \frac{4ac}{4a^2} = 0$$

$$\left(x + \frac{b}{2a} \right)^2 = \frac{\Delta}{4a^2} \in \mathbb{C} \quad \text{avec} \quad \Delta = b^2 - 4ac$$

$$\exists z_1, z_2 = -z_1 / z_1 = -z_2 = \frac{\Delta}{4a^2}$$

$$x + \frac{b}{2a} = \pm z_1$$

$$x = -\frac{b}{2a} \pm z_1$$

- 001 Nombres et probabilités (cours)
- 1 Ensemble \mathbb{N} des entiers naturels
 - 2 Principes des systèmes de numération
 - 3 Étude de l'anneau $(\mathbb{Z}, +, \times)$.
 - 4 Étude de l'ensemble $\mathbb{Z}/n\mathbb{Z}$
 - 5 PGCD
 - 6 PPCM
 - 7 Nombres premiers
 - 8 Ensemble des réels \mathbb{R}
 - 9 Nombres complexes

≈ 1952 A Boulouris. (Mme Manotti en 1956)

1962 Lycée S^r Exupéry à S^r Raphaël